Universidade de Aveiro Departamento de Engenharia Mecânica
2017

Samuel Fernando
Jorge Calçado

Automatização e controlo de reservas na indústria hoteleira

Universidade de Aveiro Departamento de Engenharia Mecânica
2017

Samuel Fernando
Jorge Calçado

Automatização e controlo de reservas na indústria hoteleira

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestrado em Engenharia Mecânica, realizada sob orientação científica de José Paulo Oliveira Santos, Professor Auxiliar do Departamento de Engenharia Mecânica da Universidade de Aveiro.

Apoio financeiro dos projetos UID/EMS/00481/2013-FCT e CENTRO-01-0145-FEDER-022083

O júri / The jury

Presidente / President

Prof. Doutor Miguel Armando Riem de Oliveira
Professor Auxiliar da Universidade de Aveiro

Vogais / Committee

Prof. Doutor José Paulo Oliveira Santos
Professor Auxiliar da Universidade de Aveiro (Orientador)

Prof. Doutora Ana Maria Pinto de Moura
Professora Auxiliar da Universidade de Aveiro (Arguente Principal)

Agradecimentos / Acknowledgements

Gostaria de agradecer em primeiro lugar aos meus pais e família por me terem ajudado sempre em tudo o que necessitei. Queria também agradecer à minha namorada e ao meu irmão por todo o apoio que me têm dado no decorrer da realização deste trabalho. Ao Professor Doutor José Paulo Oliveira Santos, queria deixar os meus agradecimentos pelo apoio, disponibilidade e paciência na realização desta dissertação. Por fim agradeço aos meus amigos e colegas de curso que direta ou indiretamente me apoiaram durante todo o percurso académico.

Palavras-chave ESP8266; Base de Dados; Servidor WEB; Plataforma WEB; etc.

Resumo

Esta dissertação visa desenvolver um sistema de controlo e gestão de acessos para a indústria hoteleira.
O uso deste sistema destina-se a resolver alguns problemas encontrados a nível de custos de funcionamento de uma receção 24 sobre 24 horas e a nível de tempo despendido pelo cliente no *check-in*, melhorando assim o nível de conforto dos clientes no processo de reserva de um alojamento.
As soluções de mercado (evidenciadas no estado da arte), embora tenham muitas vantagens, não permitem a automação total do sistema de controlo de acessos, nem usam a mesma tecnologia de comunicação entre a fechadura da porta e o servidor WEB da plataforma proposta.
A plataforma proposta permite, além da reserva remota do alojamento (à semelhança de outras plataformas no mercado), o pagamento da reserva através de "PayPal" e o registo numa base de dados remota de todas as informações relevantes ao funcionamento do sistema. O servidor WEB também tem algumas páginas PHP que permitem a programação automática da fechadura, sem ser necessário a intervenção dos colaboradores da unidade hoteleira com todos os custos inerentes.
Todo este processo é feito pelo cliente, remotamente, através de uma plataforma WEB de reservas (como muitas no mercado) e pela própria fechadura da porta com as novas funcionalidades propostas.
O funcionamento da fechadura da porta baseia-se no uso de um teclado, um microcontrolador com uma interface Wi-Fi para comunicação com o servidor WEB do sistema, e na consequente aquisição das informações necessárias para o seu funcionamento (datas de *check-in* e *check-out*, código de acesso e a data/hora do servidor).
O administrador, ou os colaboradores das unidades hoteleiras, por sua vez, com esta solução, não precisam ir ao lugar desejado para entregar a chave do espaço, cartões, ou *tags RFID* ao cliente (*check-in*). O administrador também pode, através da plataforma de reservas, monitorizar as reservas em vigor e controlar todas as informações disponibilizadas na plataforma. Estes também podem monitorizar o momento em que a porta está aberta ou fechada (através de sensores magnéticos).
A solução proposta, além dos recursos apresentados acima, usa *hardware* com baixo custo de aquisição e de implementação em instalações existentes.
Este documento procura apresentar todas as etapas inerentes à obtenção do protótipo proposto. Este trabalho está estruturado de forma a apresentar: a pesquisa realizada em torno dos conceitos teóricos necessários, a solução proposta para resolver os problemas apresentados na introdução à dissertação, a implementação da solução com todo o *software* e *hardware* desenvolvido, as considerações finais (solução final *versus* objetivos iniciais) e sugestões para trabalhos futuros.

Keywords ESP8266; Database; WEB Server; WEB Reservation Platform; etc.

Abstract

The aim of this thesis is to develop a system of access control for the hotel industry.
The use of this system is intended to resolve some of the problems with the expense of operating a reception desk 24-hours-a-day and the time expended on client check-in, thereby improving the client's comfort during the hotel's accommodation booking process.
The state-of-the-art solutions on the market, despite having many advantages, do not allow for the total automation of the access control system nor do they use the same communication technology between the door lock and the proposed WEB platform server.
The proposed platform, aside from the remote accommodation booking (similar to other existing market platforms), also allows for the reservation payment through "PayPal" and the registration of all information related to the operation of the system on a remote database. The WEB server also has some PHP pages which permit the automatic programming of the lock without the intervention of the hotel staff with their inherent costs.
This entire process is carried out by the client, remotely, through a WEB reservation platform (like many on the market) and the door lock itself with the new proposed functionalities.
The functioning of the door lock is based on the use of a keyboard, a microcontroller with a Wi-Fi interface to communicate with the system's WEB server, and consequently acquire the necessary information for its operation (check-in and check-out dates, access codes and server date/time).
With this solution, the administrator, as well as the other hotel staff, do not need to go to the designated location to hand over room keys, cards or RFID tags to the client (check-in). Through the reservation platform, the administrator can also monitor current reservations and control all of the available information on the platform, in addition to monitoring the moment the door is opened or closed (through magnetic sensors).
The proposed solution, in addition to the characteristics outlined above, uses hardware with low costs of acquisition and implementation in existing installations.
This document seeks to show all the steps inherent in obtaining the access control system's prototype and is structured in such a way as to present the research carried out (around the theoretical concepts needed), the solution proposed to resolve the problems presented at the introduction of this thesis, the implementation of the solution with the entire software and hardware developed and, finally, the final considerations (final solution versus initial goals) and suggestions for future implementations.

Conteúdo

Lista de Tabelas

Lista de Figuras

Capítulo 1

Introdução

Este capítulo procura apresentar alguns pontos tidos em consideração na escolha do tema a desenvolver nesta dissertação. Estas considerações estão diretamente relacionadas com o impacto do Turismo na economia nacional e mundial, assim como na comodidade dos clientes e administradores no momento da reserva de determinado imóvel.

Posteriormente, é feito um levantamento do problema em estudo nesta dissertação, sendo esse o objeto de motivação no desenvolvimento deste trabalho.

Por último, apresenta-se a estrutura utilizada na escrita desta dissertação.

1.1 Enquadramento

O Turismo é considerado um sector de grande peso na economia mundial, sendo este responsável pela criação de muitos empregos. Este setor contribui para o desenvolvimento regional de zonas onde, por vezes, não existem outras alternativas para alcançar esse objetivo.

As secções seguintes procuram apresentar alguns dados retirados do INE (Instituto Nacional de Estatística) sobre as estatísticas do Turismo em 2015 (publicadas em meados de 2016). Os dados apresentados são de 2015, pois aquando da escrita deste capítulo, as informações relativas ao ano de 2016 ainda não tinham sido publicadas (as estatísticas são sempre apresentadas com um ano de atraso).

1.1.1 Turismo Internacional

A nível internacional, ao longo dos últimos anos, tem-se verificado um aumento sistemático do número de turistas. Estes valores apenas demonstram a firmeza do setor Turístico, bem como a posição relevante que este ocupa no crescimento económico de um país.

Este setor representa cerca de 9% do PIB mundial, sendo responsável por cerca de 6% do total de exportações. É também importante salientar que em cada 11 empregos, pelo menos 1 está ligado ao Turismo. Em 2015 foram registadas cerca de 1.184 milhões de chegadas de turistas, valor este cerca de 4.4% superior ao de 2014 (Ver Figura 1.1). Esta flutuação deve-se sobretudo às flutuações cambiais das moedas, forte queda do preço do petróleo e outras matérias-primas.

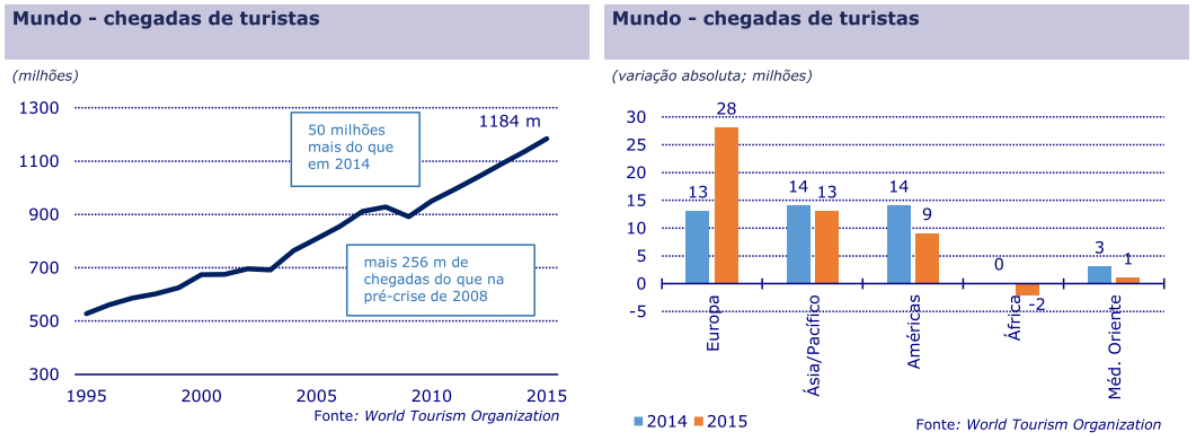


Figura 1.1: Chegada de Turistas.

A Figura 1.2 mostra, entre 2010 e 2030, uma taxa de crescimento das chegadas internacionais de aproximadamente 3.3%, atingindo valores na ordem dos 1.8 mil milhões de turistas. As tendências na procura de destinos apontam para a escolha de países emergentes/em desenvolvimento.

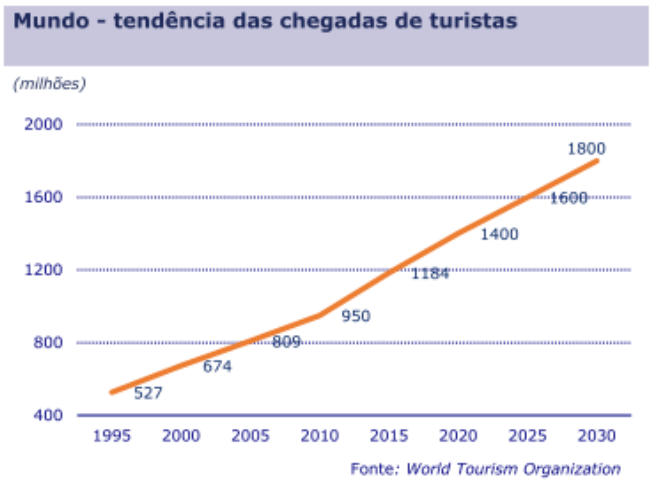


Figura 1.2: Tendências na chegada de Turistas.

Ao longo dos últimos anos, na Europa, os gastos relativos a viagens de negócio têm aumentado consideravelmente, superando os gastos relacionados com viagens de lazer. As viagens de lazer, apesar da estabilidade dos valores apresentados, apresentam gastos superiores à média mundial (Ver Figura 1.3).

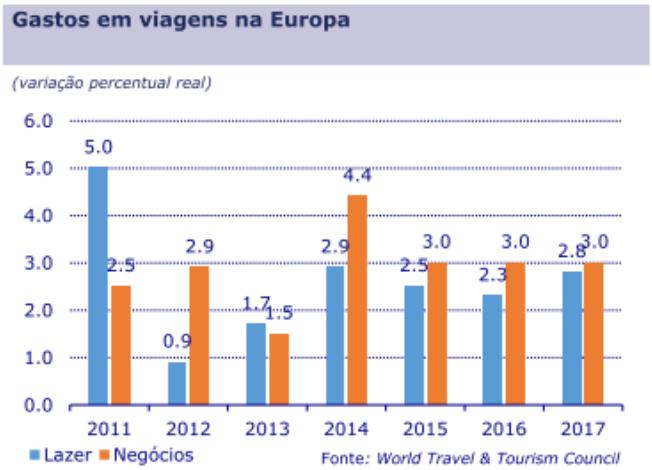


Figura 1.3: Gastos em viagens na Europa.

1.1.2 Turismo Português

Segundo o *"The Travel & Tourism Competitiveness Report"* de 2015, Portugal encontra-se bem colocado, na 15ª posição, tendo um nível de competitividade (atração) turística de 4.64.

Após a implementação do plano de ajustamento externo, devido à intensa crise económica no país, Portugal tem conseguido manter os saldos externos excedentários. Estes saldos externos são provenientes de fluxos de rendimentos que entraram em Portugal provenientes do exterior. Estes saldos dizem-se excedentários por serem superiores aos fluxos de rendimentos que saíram do país. Esta premissa constitui um elemento de suporte fundamental para investidores externos, mesmo estando o país em situação de recuperação da crise económica sofrida.

No ano de 2015 o excedente da balança de Turismo superava os 7.7 mil milhões, tendo um grande contributo para o saldo externo (Figura 1.4).

Balança Corrente - Milhões de euros

	2000	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Exportações												
Bens e serviços	36,440	42,734	49,854	54,896	56,223	47,588	54,139	61,595	64,372	68,587	70,747	74,064
Serviços	10,152	12,182	14,594	16,891	17,668	16,165	17,223	19,299	20,063	22,111	23,511	25,073
Viagens e tur.	5,720	6,199	6,672	7,402	7,440	6,908	7,601	8,146	8,606	9,250	10,394	11,362
Importações												
Bens e serviços	50,401	56,732	63,419	67,796	72,993	59,427	66,943	68,048	64,204	65,455	68,781	70,950
Serviços	6,965	7,635	8,933	9,796	10,486	9,878	10,760	11,287	10,569	10,928	12,060	12,795
Viagens e tur.	2,422	2,454	2,658	2,869	2,939	2,712	2,953	2,974	2,946	3,120	3,318	3,612
Saldo												
Balança corrente	-13,876	-15,679	-17,744	-17,089	-21,691	-18,285	-18,260	-10,572	-3,202	**2,478**	**212**	**813**
Bens e serviços	-13,961	-13,998	-13,564	-12,900	-16,770	-11,839	-12,804	-6,452	169	**3,132**	**1,965**	**3,114**
Serviços	3,187	4,547	5,661	7,094	7,182	6,288	6,463	8,012	9,494	**11,183**	**11,451**	**12,278**
Viagens e tur.	3,298	3,744	4,014	4,533	4,501	4,196	4,648	5,172	5,660	**6,130**	**7,076**	**7,750**

Fonte: Banco de Portugal.

Figura 1.4: Balança corrente.

Nos últimos anos registou-se um aumento significativo do número de dormidas em Portugal, tomando, em 2015, um valor máximo de 58.2 milhões. Grande parte desse valor encontra-se nas dormidas em estabelecimentos hoteleiros, tendo sido alcançadas 48.9 milhões de dormidas. Nos 6 anos anteriores a 2015, a taxa de crescimento desta variável foi de aproximadamente 30%, sendo este um valor considerado bastante satisfatório (Ver Figura 1.5).

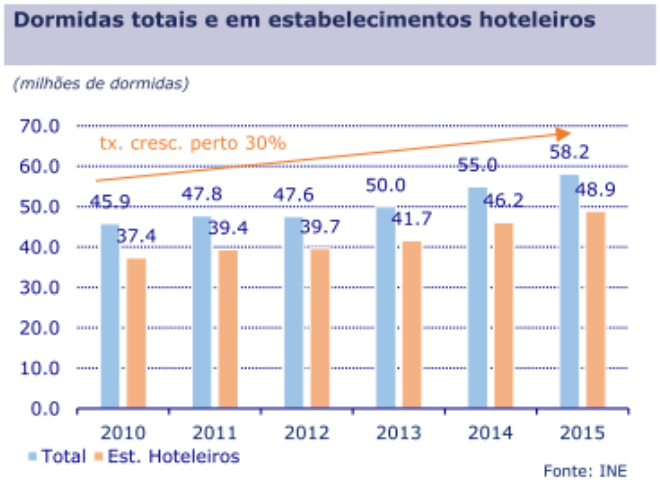


Figura 1.5: Dormidas totais vs Dormidas em estabelecimentos hoteleiros.

Em 2015, cerca de 70% das dormidas registadas foram de turistas estrangeiros, sendo os restantes 30% relativos a turistas nacionais (Ver Figura 1.6).

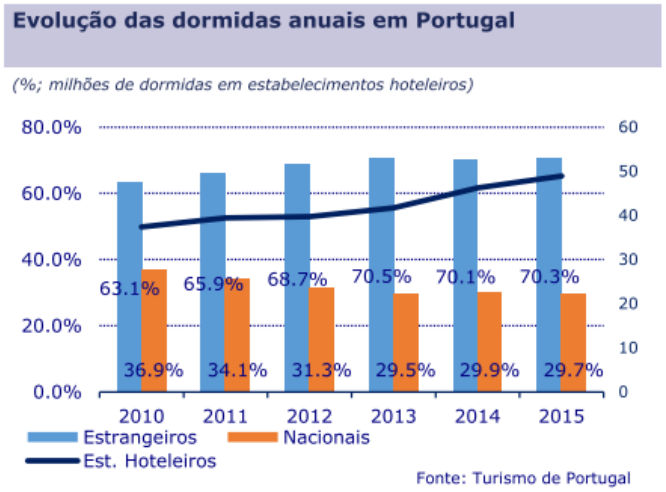


Figura 1.6: Evolução das dormidas anuais em Portugal.

Com os valores anteriormente expostos, o país optou por um aumento da capacidade de alojamento e na maior promoção no exterior, chegando a ter em 2015 312 mil camas no setor hoteleiro. Grande parte do alojamento é feito em hotéis, sendo a "menor fatia" em alojamentos rurais (Ver Figura 1.7) [1].

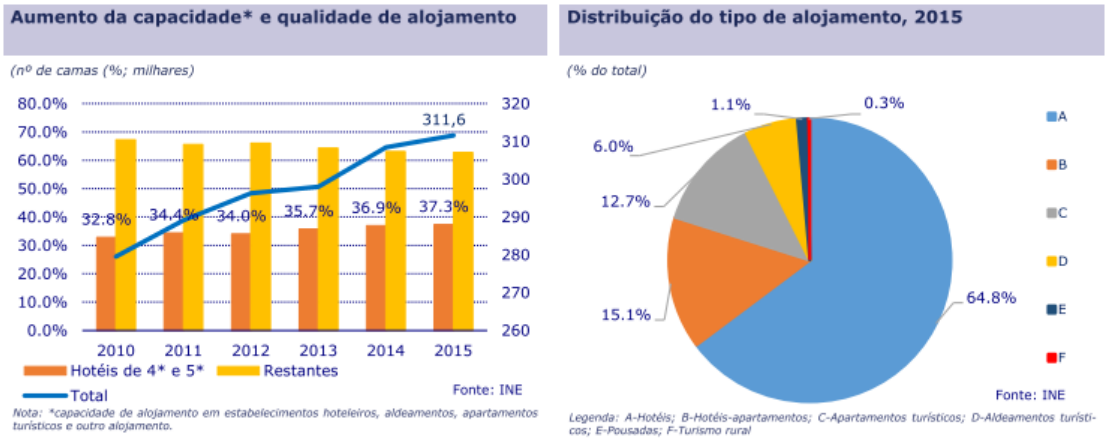


Figura 1.7: Aumento da capacidade e qualidade do Alojamento.

1.2 Motivação

Os resultados estatísticos anteriormente apresentados mostram que, em Portugal, as dormidas em estabelecimentos hoteleiros representam grande parte das dormidas registadas no país. Desta forma, foi estabelecido como mercado alvo a indústria hoteleira.

Uma receção hoteleira representa grande parte dos custos fixos associados ao funcionamento de um hotel (ou outro estabelecimento semelhante), pois exige um atendimento contínuo (24/24 horas). Assumindo que um trabalhador regular trabalha 8 horas por dia, é necessário garantir 3 turnos diários para cobrir as necessidades de atendimento.

Para além dos custos de funcionamento de uma receção, é fundamental garantir o conforto dos intervenientes no processo de aluguer de um imóvel. Todo o processo de *check-in*, a deslocação do proprietário do apartamento/moradia que se pretende arrendar, a verificação prévia do número de quartos disponíveis e do período em que o imóvel se encontra arrendado são aspetos que seriam interessantes melhorar/automatizar.

1.3 Objetivos

O objetivo desta dissertação assenta, em grande parte, na resolução dos problemas identificados na secção 1.2. Desta forma, pretende-se desenvolver um sistema capaz de monitorizar e controlar o acesso de determinado cliente ao espaço arrendado, de forma totalmente automática.

O sistema proposto tem por princípio a atribuição de um código aleatório a cada cliente, válido apenas para o período de arrendamento definido na reserva. Este sistema assenta numa solução bastante compacta e com um custo de implementação relativamente reduzido.

Todo o processo de reserva e pagamento é realizado com o auxílio de uma plataforma WEB. O *check-in* e a verificação do código de acesso são conseguidos através de um microcontrolador embutido na fechadura do espaço.

1.4 Organização

Esta secção existe com a intenção de apresentar ao leitor a estrutura seguida na escrita desta dissertação. Para além deste capítulo meramente introdutório, o documento encontra-se dividido em 6 partes essenciais, apresentadas de forma sucinta na lista seguinte:

- **Capítulo 2:** Este capítulo apresenta alguns conceitos teóricos fundamentais necessários no desenvolvimento da solução proposta. Nestes conceitos fundamentais pretende-se apresentar um pequeno resumo sobre protocolos de segurança de redes Wi-Fi, sobre as etapas e algumas normas existentes para sistemas de controlo de acessos e finalmente sobre alguns mecanismos existentes para identificação do utilizador. No fim deste capítulo são apresentadas algumas soluções comerciais de controlo de acessos em unidades hoteleiras bem como alguns sistemas propostos em dissertações e patentes registadas no INPI (Instituto Nacional da Propriedade Industrial).

- **Capítulo 3:** O capítulo 3 apresenta uma solução possível para resolução dos problemas e para consolidação dos objetivos identificados no Capítulo 1. Nesta fase é necessário ter em atenção o nível de conhecimento do leitor sobre a matéria em estudo. Dessa forma, é fundamental descrever todo o funcionamento do sistema e o tipo de comunicação esperada entre os equipamentos intervenientes no processo, de forma simples e concisa.

- **Capítulo 4:** Neste capítulo apresentam-se todas as etapas inerentes à implementação da solução, bem como todos os componentes integrantes do sistema em estudo. A descrição da solução final passa pela caracterização do software desenvolvido, juntamente com a apresentação dos componentes principais que garantem o bom funcionamento da fechadura "inteligente" do alojamento.

- **Capítulo 5:** O capítulo de Considerações Finais é constituído por um pequeno texto resumo da solução desenvolvida, juntamente com a análise crítica ao funcionamento do sistema. Em adição à informação anterior, numa perspetiva de continuidade, são apresentadas algumas sugestões de melhoria ao trabalho desenvolvido.

- **Apêndices:** Esta divisão do documento procura complementar alguma da informação dispensada nos capítulos anteriores. Esta dissertação tem na sua constituição os seguintes Apêndices:

  - **Apêndice A - Site de Reservas:** Este primeiro Apêndice mostra através de *print sreens* a interface desenvolvida para a reserva de determinado alojamento e monitorização da informação em fluxo no sistema.
  - **Apêndice B - Configuração do servidor de emails *Mercury*:** Este apêndice existe para demonstrar todo o processo necessário para a configuração do servidor de emails *Mercury*, para o envio de emails através do GMAIL (Usando o protocolo SMTP).
  - **Apêndice C - Configuração do *router* para comunicação SIM900:** Para teste da comunicação entre o SIM900 e um computador numa rede local

foi necessária uma pré-configuração do *router* da operadora de rede. Esta configuração permite o reencaminhamento de pedidos HTTP que chegam ao *router* (na porta 80), diretamente para o computador local.

- **Apêndice D - *Grafcet* da comunicação SIM900**.
- **Apêndice E - Esquema do módulo para a comunicação entre SIM900 e servidor WEB**.
- **Apêndice F - Divisor resistivo para leitura Teclado:** Este apêndice mostra o funcionamento do divisor resistivo necessário para a leitura do teclado. A utilização da porta analógica do ESP exige diferentes valores de tensão consoante as teclas pressionadas no teclado. Isto permite posteriormente a identificação das teclas por comparação entre o valor "teórico" e o valor obtido no momento do pressionar da tecla.
- **Apêndice G - Esquemas Elétricos das placas PCB**.

Capítulo 2

Revisão do Estado da Arte

Este capítulo pretende ilustrar alguns dos conhecimentos adquiridos durante o desenvolvimento da solução proposta nesta dissertação.

Toda a informação apresentada nesta secção relaciona-se diretamente ou indiretamente com o tema "Controlo de Acessos" e divide-se em 5 elementos principais:

- Apresentação do conceito de IOT (*Internet Of Things*);
- Etapas e Normas existentes no Controlo de Acesso a determinada entidade;
- Protocolos de Segurança em redes Wi-Fi;
- Mecanismos para identificação do utilizador e soluções existentes no mercado (soluções à venda, dissertações e patentes);

O capítulo termina com uma pequena análise crítica aos mecanismos de controlo de acesso apresentados. Esta análise tem por objetivo a escolha do método ideal a implementar no sistema proposto.

2.1 IOT - *Internet of Things*

O conceito "*Internet Of Things*", também conhecido por IOT, define uma revolução tecnológica que tem por princípio permitir a interação entre diversos equipamentos presentes no quotidiano de cada utilizador. Esta interação fomenta a comunicação entre equipamentos, utilizadores e aplicações existentes. O "criador" deste conceito, Kevin Ashton, referiu numa entrevista que anteriormente à dita "IOT" os computadores poderiam ser equiparados a pessoas sem capacidades de aprendizagem, ou seja, que apenas sabiam aquilo que lhes era ensinado. Essa observação pode ser vista como uma grande limitação, pois com a quantidade de informação disponível na WEB, o registo manual dessa informação em tempo real torna-se completamente impossível.

Além disso, a informação registada manualmente acarreta erros de introdução que podem levar a posteriores erros de análise e tratamento de dados [2].

Atualmente, esta definição tem sido aplicada em muitos projetos que visam a transformação de algo tipicamente básico em algo inteligente. Um dos exemplos mais conhecidos consiste em tornar uma habitação numa "Casa Inteligente", em que todos os equipamentos domésticos têm capacidade de acesso à Internet, permitindo assim o seu controlo e

monitorização através de um telemóvel ou de outro equipamento semelhante. A imagem seguinte (Figura 2.1) mostra um exemplo de uma "Cidade Inteligente", em que tudo é monitorizado e controlado de forma a reduzir ao máximo o desperdício, e assim tornar a cidade o mais eficiente possível [3].

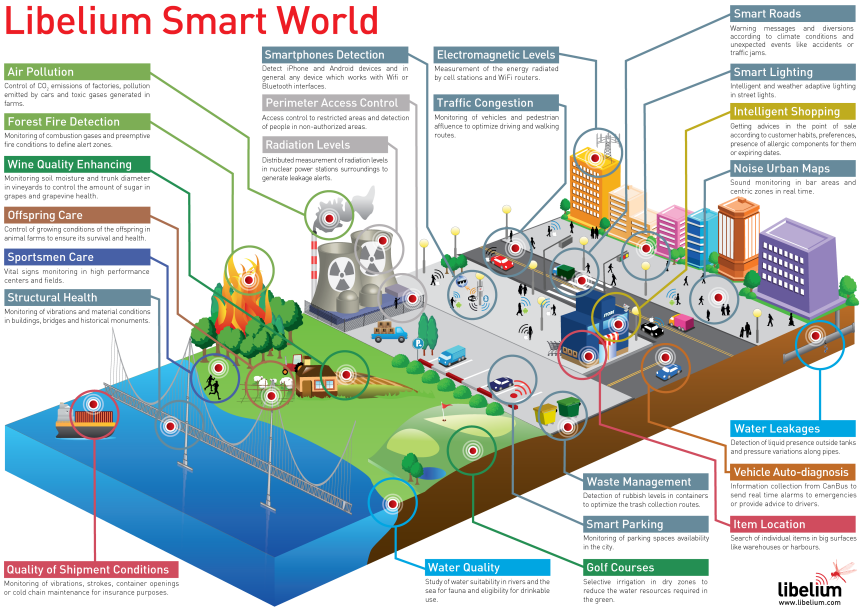


Figura 2.1: IOT - Smart City [3]. (Adaptada)

A aplicação da IOT na indústria pode trazer benefícios a nível de aumento de produção e automatização de todos os processos inerentes, desde a conceção da ideia até à obtenção do produto final. Outra indústria que pode favorecer da aplicação deste conceito é a indústria médica. A utilidade de ter equipamentos que permitem a comunicação através da Internet reside na monitorização de doentes ou até mesmo na antecipação de possíveis casos clínicos mais complicados. Estas medidas podem contribuir para um aumento significativo da esperança média de vida.

Na aplicação desta ideologia, é necessário ter em conta a segurança da informação presente no fluxo de dados entre equipamentos. O acesso ilegal a essa informação pode ter consequências muito graves a nível económico, ambiental ou até mesmo a nível de segurança do utilizador [4].

2.2 Controlo de acessos

O controlo de acessos define o nível de autorização que determinado utilizador tem (ou não) na tentativa de acesso a determinado espaço. Os níveis de autorização dos utilizadores são-lhes atribuídos por um elemento de entidade superior, ou até mesmo pelo próprio proprietário do espaço desejado.

O controlo de acesso físico pode ser controlado por um guarda ou rececionista, por um meio mecânico (fechadura), ou através de meios tecnológicos (cartões RFID, teclado alfanumérico, entre outros).

O controlo de acessos é um ramo da segurança que permite controlar a forma como os utilizadores/sistemas interagem entre si. Os sistemas existentes para controlo de acessos permitem a proteção de informação confidencial, proteção de sistemas físicos de acesso não autorizado, assim como a determinação do nível de autorização de cada utilizador. Desta forma, cada utilizador tem de passar por um conjunto de etapas essenciais, precedentes ao acesso à entidade pretendida. Tendo em consideração o número de entidades que podem ter interesse no acesso a determinada informação/espaço, é necessário pré-estabelecer uma definição clara de sujeito e objeto no contexto de controlo de acessos.

O acesso em si é definido como o fluxo de informação que decorre entre um sujeito e um objeto. Um sujeito é quem solicita o acesso a um objeto, ou aos dados que este contém. Um sujeito pode ser um utilizador, um programa ou processo que tenta aceder a um objeto para concretizar uma dada tarefa. Quando, por exemplo, um programa acede a um determinado ficheiro, o programa é o sujeito e o ficheiro o objeto. Um objeto define-se como uma entidade passiva que contém a informação necessária/funcionalidade requerida. Um objeto pode ser um computador, uma base de dados, um ficheiro, um programa, entre outros. Por exemplo, na pesquisa de informação numa base de dados, quem procura é o sujeito, sendo, por isso, a base de dados o objeto passivo.

Um exemplo de controlo de acessos bastante comum nos dias de hoje assenta na utilização de um sistema de verificação de identidade com "*username*" e "*password*" no acesso a um computador ou telemóvel. O controlo de acessos permite, às organizações, a capacidade de controlar, restringir, monitorizar e proteger a disponibilidade, a integridade e a confidencialidade de determinada informação/espaço.

O acesso a determinado objeto tem de ser autorizado, de forma a respeitar as normas de segurança predefinidas, impedindo ou aceitando o acesso de alguns utilizadores conforme o seu nível de autorização. Desta forma, o acesso a determinada entidade encontra-se dividido em 4 etapas principais: a identificação, a autenticação, a autorização e a auditoria.

2.2.1 Etapas de controlo de acessos

Para poder aceder a determinado objeto, o utilizador tem que verificar uma série de requisitos, que vão desde confirmar a sua identidade, a ter consigo as credenciais de identificação necessárias, bem como ter autorização para efetuar o pedido de acesso que pretende. Após esta verificação ser concluída com sucesso, o requerente pode usufruir do espaço/informação que deseja, não esquecendo que uma autoridade de nível superior pode sempre monitorizar a sua atividade.

Identificação

A identificação é utilizada para assegurar que um sujeito (requerente) é quem diz ser. Para isto, cada utilizador possui um "*username*"/"*account number*" que o identifica.

Autenticação

A autenticação de determinado utilizador consiste na apresentação de uma "*password*", ou algo semelhante, para confirmação dos dados de identificação previamente introduzidos.

Este dados são posteriormente comparados com a informação registada na base de dados, relativa ao utilizador identificado na etapa anterior.

Na eventualidade da informação introduzida coincidir com a informação registada na base de dados, o utilizador pode considerar-se autenticado.

Autorização

Concluídas as etapas anteriores, existe a necessidade de verificar se o utilizador que requer o acesso ao espaço/informação pretendido(a) tem autorização por parte do administrador para aceder ao pedido. Esta confirmação é conseguida através de uma comparação das credenciais do sujeito com os níveis de autorização que cada utente da organização possui.

Auditoria

A auditoria consiste na monitorização da atividade do utilizador. Esta ferramenta permite fortificar as políticas de segurança, podendo também ser utilizada como ferramenta de investigação dos movimentos que os utilizadores efetuam após o seu registo. O registo destas atividades permite à organização detetar o acesso por parte de intrusos ao sistema, controlar as ações que os utilizadores realizam, disponibilizar conteúdo adequado ao nível de autorização de cada sujeito, entre outros [5][6].

2.2.2 Norma EN50131

A implementação de uma solução de segurança requer a verificação prévia do cumprimento dos padrões estipulados na norma europeia EN50131.

Esta norma define um conjunto de regras para equipamentos de alarme e intrusão. As instalações podem classificar-se segundo 4 graus de risco, sendo este um ponto considerado interessante para o caso em estudo. As instalações podem, assim, classificar-se em:

Grau 1: Baixo risco
Instalações na qual a probabilidade de acesso por utilizadores não autorizados é muito pequena. As intrusões neste tipo de edifícios são feitas através de portas ou janelas.

Grau 2: Risco baixo a médio
Este tipo de risco engloba a maioria dos sistemas residenciais ou instalações comerciais de baixo risco. Neste caso os intrusos não possuem grandes conhecimentos acerca dos sistemas de segurança e têm recursos limitados. O acesso às instalações é conseguido através de pontos desprotegidos.

Grau 3: Risco médio a elevado
Nesta categoria encontram-se inseridas a maioria das instalações industriais e comerciais. Os intrusos, nesta situação, têm experiência com o equipamento necessário para lidar com os sistemas de deteção de intrusão mais simples.

Grau 4: Risco elevado
Esta categoria inclui instalações de alta segurança e com conteúdo de elevado valor. Os ataques a estes estabelecimentos são realizados por indivíduos com elevado conhecimento sobre mecanismos de segurança e equipados com tecnologia de ponta.

Por norma, os sistemas de segurança assentam em 3 pilares fundamentais: as pessoas, a tecnologia e o processo. Para assegurar um nível de proteção adequada, é necessário garantir o equilíbrio entre estes três fatores. É importante salientar que a intervenção humana é indispensável nesta associação, não esquecendo o possível erro que isso acarreta [7].

Um profissional que trabalha com segurança de informação tem de possuir um certificado que lhe atribui capacidades para saber como proteger dados e informação confidencial da organização que o contrata. Esta preocupação tende a aparecer cada vez mais devido aos elevados riscos de acesso indesejado a informação registada num computador. Esse certificado é denominado de CISSP (*Certified Information Systems Security Professional*), e engloba diversas áreas de segurança, das quais faz parte o controlo de acesso [5].

2.3 Segurança de redes Wi-fi

As redes sem fios, nomeadamente as redes 802.11 - mais conhecidas por WLAN (*Wireless Local Area Network*) ou por redes Wi-Fi (*Wireless Fidelity*), são atualmente bastante utilizadas na transferência de dados entre equipamentos. Wi-Fi é uma marca licenciada pela *Wi-Fi Alliance* para catalogar a tecnologia inerente a redes sem fios baseadas nos padrões 802.11 da IEEE.

Apesar da inexistência de cabos na comunicação entre dispositivos, as redes sem fios trazem diversos problemas de segurança quando comparadas a soluções cabladas.

A utilização não autorizada do sinal das redes sem fios, ou nos próprios *access point* que as difundem, comprometem a fiabilidade da comunicação entre equipamentos.

Para contornar este problema existem mecanismos de segurança capazes de assegurar a autenticação dos utilizadores, assim como a confidencialidade e autenticidade dos dados enviados/recebidos.

2.3.1 WEP - *Wired Equivalent Privacy*

Este protocolo foi o primeiro protocolo de segurança desenvolvido para redes 802.11. Este permite a autenticação dos equipamentos, bem como a confidencialidade e controlo de integridade dos dados trocados na sua comunicação com o *access point*.

O WEP define dois modelos de autenticação no acesso a um *access point*:

- **OSA** (*Open System Autentication*): Neste modelo não existe qualquer autenticação dos equipamentos. A associação dos equipamentos ao *access point* é sempre autorizada.
- **SKA** (*Shared Key Autentication*): Neste modelo deve existir uma chave partilhada denominada de PSK (*Pre-Shared Key*) que permite a autenticação entre o equipamento e o *access point*. Esta autenticação é conseguida com o envio de uma mensagem para o equipamento. Este deve posteriormente responder com a mesma mensagem (encriptada), juntamente com a chave partilhada.

Por norma, cada *access point* permite associar quatro chaves a cada SSID (Service Set IDentifier), ou apenas uma chave ao endereço MAC (Media Access Control) de cada equipamento. O SSID indica o nome de uma rede sem fio, sendo útil no momento de

ligação à rede. O endereço MAC por sua vez é o endereço de controlo de acesso da placa de rede de um equipamento.

Apesar do método de autenticação ser definido pelo *access point*, quem escolhe o método que pretende utilizar no início do protocolo de autenticação é o equipamento que se pretende ligar. Assim sendo, inicialmente o equipamento envia um pedido de *Authentication Request*, indicando o modo de autenticação que pretende, devendo o *access point* responder com uma mensagem de erro, na eventualidade de não permitir esse modo. Caso seja permitido, seguem-se as mensagens de *Authentication Response* necessárias para a conclusão do protocolo. No modelo OSA, a mensagem de *Authentication Response* consiste, por si só, uma autorização de acesso, indicando uma autenticação bem sucedida.

No modelo SKA, pelo contrário, cada *access point* envia um desafio com um conjunto de *bits* para o equipamento de destino. O equipamento, ao receber o desafio, reenvia-o com a proteção WEP associada. Esta troca de informação permite a encriptação do desafio com uma chave PSK. Esta chave tem de ser igual no equipamento de destino e no *access point*. Após a desencriptação da mensagem, o *access point* compara o que recebeu com o que enviou. Na eventualidade da mensagens trocadas serem iguais, *access point* responde com uma mensagem de *Authentication Response* com a autorização de acesso pretendida.

Com isto, a autenticação com SKA torna-se bastante insegura, por dar a oportunidade de interceção das mensagens com o desafio enviado e a sua respetiva resposta. Com estes dados, é assim possível calcular os valores necessários para, daí em diante, o *hacker* poder autenticar-se corretamente.

É habitual os *access points* permitirem outras formas de autenticação e autorização de diversos equipamentos. Uma dessas formas consiste na ligação ao *access point* conhecendo de antemão o seu SSID. Outra forma utiliza uma lista de endereços MAC de equipamentos autorizados a estabelecer ligação com um dado *access point*.

Contudo, estes meios de proteção são ineficazes perante um atacante motivado, pois existem sempre formas de contornar estas limitações. Apesar disso, o risco é menor ao usar estas funcionalidades num ambiente mais restrito, com um número de equipamentos reduzido e estável ao longo do tempo.

No que diz respeito à confidencialidade e controlo de integridade dos dados enviados, o WEP limita-se a explorar canais de comunicação seguros. Esta confidencialidade e controlo de integridade limitam-se a mensagens *unicast* (um para um), sendo que outro tipo de mensagens - *multicast* (um para muitos) e *broadcast* (um para todos) - não se encontram abrangidas por este tipo de proteção.

Estes canais são controlados por uma PSK entre os intervenientes. O WEP não contempla a geração de novas chaves para cada associação diferente entre o equipamento e o *access point*. Assim, nessa associação, caso o *access point* tenha de usar WEP para interagir com o equipamento, este seleciona a PSK correta associando-a ao SSID ou ao endereço MAC do equipamento de destino. A comunicação segura com o WEP e a autenticação SKA podem ser escolhidas independentemente, sendo que, quando usadas simultaneamente, partilham a mesma PSK para fazer encriptações e desencriptações.

No WEP são usados dois mecanismos relevantes: um de encriptação contínua (denominado de RC4) e um de controlo de integridade dos dados recebidos (baseado no algoritmo CRC-32). Este protocolo de segurança segue uma sequência lógica de operações que são apresentadas de seguida:

1. Para cada mensagem é escolhido um vetor de iniciação (VI);
2. O VI, juntamente com a chave pré-partilhada WEP, utilizam o algoritmo de encriptação RC4 para gerar uma chave contínua;
3. A chave contínua gerada no ponto 2 é somada aos dados a enviar e ao resultado da soma gerada com o algoritmo de controlo de integridade CRC-32 (soma denominada de ICV - *Integrity Check Value*). A soma do conjunto é denominada criptograma;

   Após o envio deste criptograma, a sua desencriptação segue na ordem seguinte (inversa à anterior):

4. Recetor retira o VI da mensagem recebida;
5. Após o VI ser retirado, este é utilizado juntamente com a chave WEP para gerar uma chave contínua;
6. A chave contínua é somada ao criptograma recebido. Do resultado dessa soma resultam os dados inicialmente apresentados para a encriptação e o respetivo ICV.

A integridade dos dados recebidos é verificada comparando o ICV extraído da mensagem com o ICV calculado a partir dos dados obtidos após a desencriptação.

A chave WEP usada na encriptação e desencriptação de mensagens WEP consiste numa PSK - que pode estar associada ao endereço do recetor (na encriptação) ou ao endereço do emissor (na desencriptação) - ou numa chave de conjunto de quatro PSK pré configuradas no *access point*, que podem ser usadas por qualquer equipamento que se pretenda associar a ele.

No primeiro caso, existe a possibilidade de atribuir uma chave personalizada para cada associação feita entre o *access point* e o equipamento. Essa configuração pode ser feita no *access point* com um mapeamento do endereço MAC do equipamento.

No segundo caso, as diferentes PSK usadas são identificadas por um valor (*Key ID*) enviado na mensagem entre o VI e os dados encriptados. Na configuração do equipamento associado ao *access point* deve ser indicada tanto a chave do WEP como o *Key ID* utilizado.

Na versão inicial do WEP, o gerador de chave contínua RC4 funcionava com chaves de 64 *bits* - 40 *bits* da chave de encriptação e 24 *bits* correspondentes ao VI. A chave de encriptação, por ter apenas 40 *bits*, fornece uma segurança pouco eficaz face a ataques externos. Ao longo dos tempos, foram surgindo soluções com chaves de encriptação até 232 *bits*, que contribuíram para um aumento significativo da robustez do WEP.

Este protocolo, por ter sido o primeiro a ser desenvolvido, apresenta algumas falhas que podem comprometer a segurança dos dados enviados. Um dos problemas do WEP assenta na inexistência de soluções que permitam gerar novas chaves WEP a cada vez que um equipamento se liga a um determinado *access point*. Outro problema está presente no vetor de iniciação. Como este vetor tem um tamanho reduzido, ou seja, um número finito de *bits*, ao fim de algumas associações entre diferentes equipamentos e o *access point*, a repetição de chaves WEP é inevitável. Essa repetição irá limitar o número possível de criptogramas existentes, sendo fácil, ao fim de algum tempo, desencriptar o conteúdo das mensagens.

As vulnerabilidades deste protocolo levaram ao desenvolvimento de um mecanismo de segurança mais complexo, tendo sido posteriormente aplicado algoritmo de encriptação AES nas concretizações do 802.11i (WAP2), tanto na encriptação, como no controlo de integridade das mensagens. Esta mudança apresenta grandes desvantagens na sua implementação, pois não permite o uso dos equipamentos de rede até então utilizados.

A forma de contornar este problema assentou no desenvolvimento de uma solução intermédia, menos complexa que o WAP2, mas, no entanto, mais segura que o WEP - o WPA. O WPA, apesar de permitir reutilizar os equipamentos de rede dos equipamentos móveis que suportam o WEP, exige que os access point saibam operar com o WPA. Este último, para além da vantagem apresentada, também oferece configurações de segurança mais simples e interessantes para ambientes mais pequenos.

2.3.2 WPA - Wi-Fi *Protected Access*

O WPA foi um protocolo intermédio que contribuiu para a resolução de alguns problemas do WEP. Apesar do WPA manter toda a parte relativa ao WEP, acrescentou algumas funcionalidades a nível de capacidade de gestão das chaves de encriptação e a nível de controlo de integridade das mensagens.

No protocolo WPA, cada mensagem é codificada com uma chave WEP diferente, reduzindo, assim a probabilidade de se construirem dicionários de chaves contínuas, mesmo na situação de ser utilizada a mesma PSK várias vezes. Outra funcionalidade relevante prende-se junto do controlo de integridade do WEP (sendo agora mais abrangente), ao ser permitido englobar campos da mensagem até então não contemplados. O controlo de integridade também deixou de ser por mensagens isoladas, e passou a ter em consideração a própria ordem das mensagens. Neste protocolo, também é importante salientar que a autenticação de utilizadores é feita com a autenticação simultânea dos equipamentos, dos *access point* e com a distribuição de chaves de sessão.

Na comunicação entre equipamentos, o WPA pode ser implementado em *software* pelos sistemas operativos, ou, em alternativa no *hardware* das interfaces de rede. No primeiro caso, a implementação pode trazer custos adicionais a nível de processamento. Este custo pode ser posteriormente abatido com a aplicação direta do protocolo nas interfaces de rede.

Esta mudança permitiu a implementação do WPA nos diversos equipamentos da rede, sem acrescentar grandes custos a nível de mudança de *hardware*. Apesar da reutilização dos equipamentos, a aplicação do protocolo WPA implica alterações no *firmware* utilizado nos *access points* (o que pode levar à troca do próprio *access point*).

Este protocolo assenta em dois pilares: o TKIP (*Temporal Key Integrity Protocol*) e o 802.1X.

O primeiro consiste num protocolo que, na sua génese, possui o WEP, usando-o sem expor as suas vulnerabilidades. Este utiliza um VI de 48 *bits*, TSC (TKIP *Sequence Counter*), que incrementa um valor, sempre que é produzida uma mensagem protegida por WEP. Esta funcionalidade permite, assim, o controlo da ordem na receção. Cada equipamento, ou *access point*, possui um TSC para cada chave TK relativa a uma associação. Este protocolo utiliza chaves WEP diferentes para cada mensagem e em cada sentido de comunicação. No TKIP, as chaves fracas do RC4 são automaticamente excluídas e o controlo de integridade das mensagens é feito com auxílio de um valor MIC (*Message Integrity Code*), calculado para cada mensagem, tendo em consideração o seu

cabeçalho. Na eventualidade de existirem valores MIC errados, são acionadas algumas contra-medidas predefinidas.

O TKIP assenta no uso de três chaves partilhadas: uma chave para confidencialidade - TK (Temporal Key) de 128 *bits* - e outras duas para controlo de integridade - chaves MIC de 64 *bits* cada, uma para cada sentido de comunicação. No entanto, o TKIP pode ser utilizado com as chaves PSK anteriormente referidas, tal como no WEP. Neste caso, as chaves podem ser calculadas diretamente a partir da PSK. Este processo tem o nome de WPA-PSK.

O segundo pilar, 802.1X, é usado para efetuar a autenticação mútua entre os interlocutores (Suplicante - equipamento que se tenta ligar à rede; Autenticador - elemento que controla o estado do terminal de acesso desse equipamento à rede; Servidor de autenticação - conduz o processo de autenticação mútua), o equipamento móvel usado e a rede, no momento em que o equipamento tenta estabelecer ligação à rede Wi-Fi. Este protocolo também serve para criar e distribuir chaves novas aos equipamentos que tentam comunicar através da rede. Numa rede sem fios os interlocutores tomam os papeis seguintes:

- Suplicante: Equipamento Móvel;
- Autenticador: *access point*;
- Servidor de Autenticação: Elemento fornecido pela ligação cablada ao *access point* (Servidor RADIUS).

2.3.3 WPA2 (802.11i)

O WPA2 é o mais complexo dos 3 protocolos apresentados para as redes 802.11. Este protocolo consiste na junção do WEP com os mecanismos utilizados pelo WPA. O WPA2 junta ainda aos protocolos anteriores o algoritmo de encriptação AES e a proteção de mensagens com AES-CCMP. Esta proteção de mensagens combina os mecanismos de segurança do 802.11i com o algoritmo de encriptação AES, utilizando chaves e blocos de dados de 128 *bits*. O AES-CCMP usa um modo de operação chamado CCM (*Counter with CBC-MAC*), que permite fornecer simultaneamente autenticação e controlo de integridade, com matrizes de encriptação por blocos de 128 *bits*.

Para enquadrar todos estes mecanismos, utiliza-se o conceito de RSN (*Robust Security Network*). Uma rede RSN tem de suportar:

- Uma autenticação mais eficaz dos interlocutores;
- Uma distribuição e melhor gestão de chaves de sessão (baseados em 802.1X);
- Mecanismos de proteção de mensagens baseados no AES/TKIP.

Pode assim concluir-se que uma rede RSN suporta os mecanismos do WPA e os mecanismos introduzidos pelo WPA2. Existe também o conceito de rede pré-RSN, que reúne os pressupostos originais de segurança definidos no 802.11.

Uma rede TSN (*Transition Security Network*) suporta simultaneamente as redes pré-RSN e RSN. Esta rede não suporta os mecanismos introduzidos pelo WPA2 [8].

2.4 Norma RS232

O protocolo utilizado, nesta dissertação, para a comunicação entre equipamentos, consiste no protocolo de comunicação RS232 (Recomendação para *Standard* 232).

Este protocolo tem por objetivo permitir a comunicação entre equipamentos digitais e redes públicas analógicas (por exemplo: ligação de computadores ou outros terminais à rede telefónica), utilizando, para isso, os chamados*modems*.

Este protocolo foi inicialmente proposto pela "Electronic Industries Association" (EIA), sendo conhecido por EIA-232.

É importante referir que a norma EIA-232D apenas indica a interface entre cada recurso e o seu respetivo *modem* (por exemplo: significado e utilidade dos pinos das fichas DB25 - Figura 2.2). Assim sendo, para interligar fisicamente recursos que se encontrem suficientemente próximos um do outro, apenas é necessário ligar diretamente as suas portas série, sem recorrer a um *modem* intermediário.

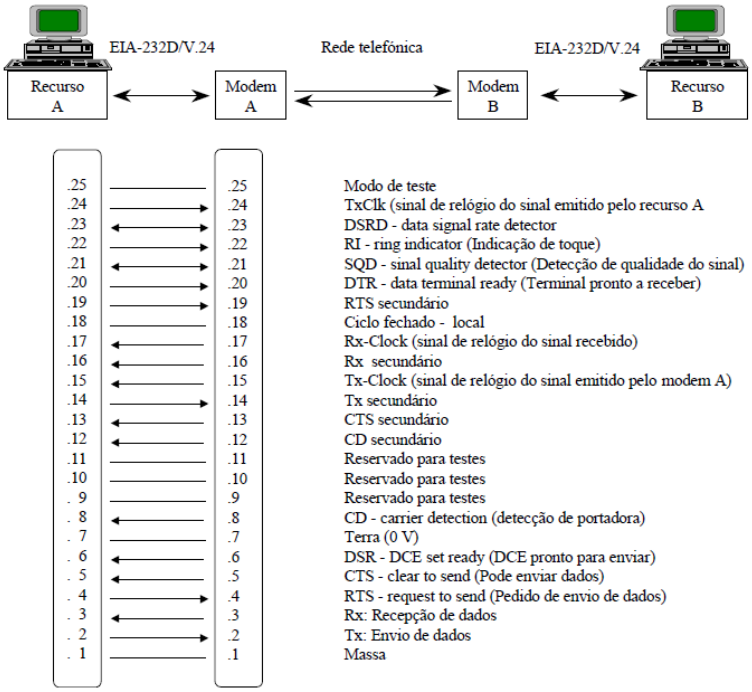


Figura 2.2: Protocolo RS232.

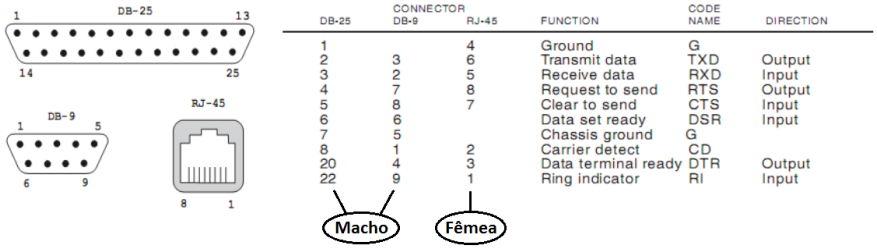
Os *modems* têm a capacidade de converter sinais digitais em sinais analógicos, o que facilita a troca de informação a grandes distâncias, utilizando a linha analógica da rede telefónica. Esta conversão acontece, pois os sinais analógicos, com a frequência adequada, conseguem percorrer distâncias superiores e com menor atenuação e distorção que os sinais digitais.

Os pinos Tx e Rx da ficha DB25 (Figura 2.3) permitem o envio e a receção de dados. Os outros pinos são utilizados para controlar:

- O início e o fim da ligação;
- O fluxo de dados da comunicação;

- O sincronismo do recurso A com o *modem* A.

O pinos secundários desta ficha existem na eventualidade de acontecer uma troca de informação, em simultâneo, utilizando a mesma interface.



CONNECTOR DB-25	CONNECTOR DB-9	CONNECTOR RJ-45	FUNCTION	CODE NAME	DIRECTION
1		4	Ground	G	
2	3	6	Transmit data	TXD	Output
3	2	5	Receive data	RXD	Input
4	7	8	Request to send	RTS	Output
5	8	7	Clear to send	CTS	Input
6	6		Data set ready	DSR	Input
7	5		Chassis ground	G	
8	1	2	Carrier detect	CD	
20	4	3	Data terminal ready	DTR	Output
22	9	1	Ring indicator	RI	Input

Figura 2.3: Fichas DB25, DB9 e RJ45 (EIA232).

A versão D da norma EIA-232 prevê dois tipos de comunicação entre equipamentos: a comunicação síncrona e assíncrona. A comunicação assíncrona indica que o sinal gerado pelo emissor, ou seja, o instante da transição do sinal (de 0 para 1 e de 1 para 0), apenas depende do seu relógio interno.

A comunicação síncrona, por sua vez, afirma que tanto o emissor como o recetor dependem do mesmo sinal de relógio para determinar os instantes de transição do sinal de dados. Neste modo, para além dos pinos Tx e Rx, também são necessários os pinos "TxClock" e "RxClock" para a sincronização do emissor e do recetor.

O protocolo RS232 não segue uma forma geométrica para a ligação física dos equipamentos, pois este define uma ligação ponto a ponto entre apenas dois equipamentos (e não uma rede de comunicação).

A transferência de *bits* entre dois equipamentos, no caso do protocolo RS232, é feita com auxílio de sinais elétricos.

Ao aplicar uma tensão positiva entre 5 e 25V, é enviado um *bit* com o valor lógico "0", sendo que uma tensão negativa entre os -5 e -25V permite enviar um *bit* com valor lógico "1".

Os sinais RS232 são gerados a partir de tensões TTL (*Transistor Transistor Logic*). Estas tensões apenas podem assumir os valores 0 ou 5V. Sendo assim, é necessário converter, posteriormente, estas tensões nas tensões suportadas pelo protocolo (Figura 2.4).

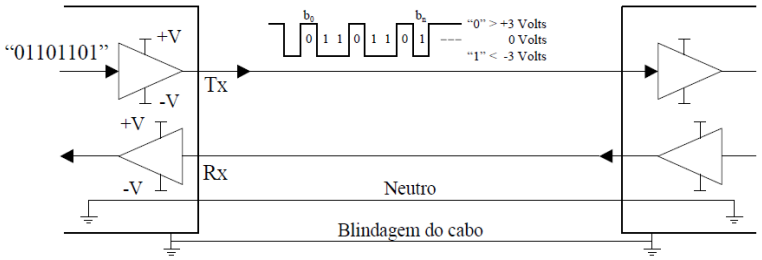


Figura 2.4: Conversão TTL para RS232.

Este protocolo, para além da informação anterior, também define o tempo que o emissor deve manter a tensão constante (positiva ou negativa), por cada *bit* enviado (*bit*

time). Quanto mais pequeno for o *bit time*, maior é o número de *bits* que o emissor pode enviar (por segundo). A este dado dá-se o nome de *baudrate* (taxa de transferência). Os *baudrates* definidos no RS232 são: 150, 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600 e 115200 *bits*/s.

Na Figura 2.5 é possível visualizar que, para uma taxa de 9600 *bits*/s, é necessário aplicar uma tensão de -5V durante (1/9600)s (um *bit time*) para enviar um *bit* com valor lógico "1".

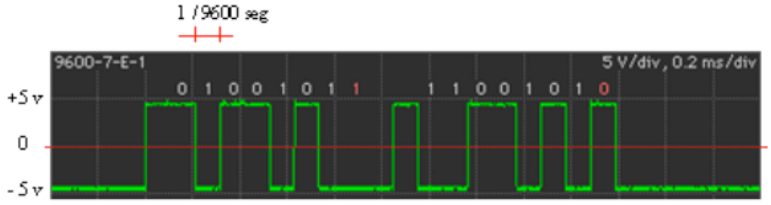


Figura 2.5: Sinais elétricos de uma comunicação RS232.

O envio de uma mensagem via RS232 é feito com auxílio de palavras série. Estas palavras são constituídas por um "start bit", 5 a 8 "bits de dados", um "bit de paridade" e um "stop bit" (Ver Figura 2.6).

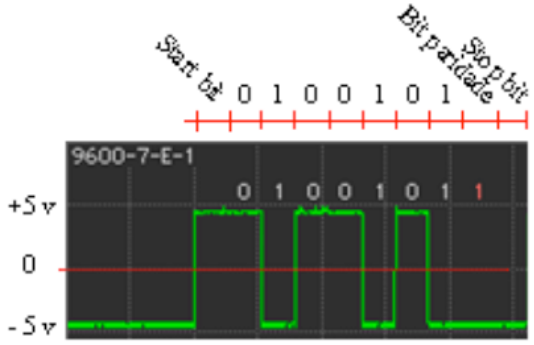


Figura 2.6: Palavra Série RS232.

Como se pode visualizar na Figura 2.6, o "start bit" corresponde a uma tensão positiva aplicada durante um *bit time*. O "bit de paridade" é opcional, e pode assumir a categoria par ou ímpar. Este *bit* também é utilizado na deteção de erros de transmissão, sendo enviado pelo emissor e interpretado pelo recetor (necessário pré-configurar os dois equipamentos para uma comunicação par ou ímpar). Na eventualidade da paridade ser par, este *bit* assume o valor "0" ou "1" por forma a garantir um número par de *bits* a "1" enviados na palavra série. O "stop bit", ao contrário do "start bit", corresponde a uma tensão negativa aplicada durante 1, 1.5 ou 2 *bit time*.

A comunicação RS232 utiliza dois fios de cobre para a transmissão de dados: um para envio e outro para receção. Dessa forma, é possível o envio e receção de dados em simultâneo, pelo que se pode concluir que o tipo de diálogo utilizado é "Full Duplex".

Existem duas formas de controlar o fluxo de dados (*Handshake*) trocados entre os equipamentos emissor e recetor. A primeira consiste no envio de uma palavra série

especial (Xoff - 0x13 hex = 00010011 bin = 19 dec). Quando o emissor receber essa palavra, suspende o envio de dados até que o recetor envie o Xon.

A segunda consiste na utilização de fios de cobre adicionais que ligam os pinos RTS (*Request to Send*) do emissor ao pino CTS (*Clear to Send*) do recetor. Quando o emissor pretende enviar dados ativa o pino RTS e o recetor, para indicar a disponibilidade em receber dados, ativa o seu pino CTS (Este controlo de fluxo é denominado de controlo de fluxo por *hardware*) [9].

2.5 Modelo Cliente/Servidor

O modelo cliente-servidor consiste numa estrutura que tem como função distribuir as tarefas e cargas de trabalho entre os fornecedores de um serviço (servidores) e os requerentes desse mesmo serviço (clientes). Neste modelo, existem três entidades envolvidas:

- **Cliente**: Entidade que requisita serviços ao servidor;
- **Servidor**: Quem partilha dados com clientes;
- **Meio de Comunicação**: Meio de comunicação entre o cliente e servidor (TCP/IP).

Os servidores destes sistemas têm um papel "central" na comunicação entre os diversos equipamentos. Estes recebem vários pedidos dos clientes e têm a função de lhes responder com a informação pretendida (Figura 2.7). Uma vez que podem ser feitas várias ligações em simultâneo entre clientes e servidor, este último tem de ter capacidade suficiente para conseguir responder às necessidades impostas. Para existir ligação entre os vários equipamentos da rede, é necessário pré-estabelecer um tipo/rede de comunicação entre os diversos equipamentos.

Figura 2.7: Esquema Modelo Cliente/Servidor.

2.6 Arquiteturas de sistema

Uma arquitetura de redes conhecida é a *peer-to-peer* (P2P). Esta arquitetura define que cada equipamento envolvente numa rede pode funcionar como cliente ou servidor, permitindo, assim, a partilha de dados sem a necessidade de um servidor central. Por definição, o sistema P2P consiste numa arquitetura de rede descentralizada. Uma vantagem deste

tipo de arquitetura assenta na ideia de não existirem equipamentos a atuar como servidor fixo, o que permite garantir a validade da rede, caso o equipamento servidor não se comporte como esperado. Na arquitetura de rede descentralizada (Ver Figura 2.8 - Esquerda), todos os equipamentos estão na mesma hierarquia, não existindo um servidor central dedicado a sustentar a comunicação entre os restantes equipamentos da rede. Para além da vantagem referida nas linhas anteriores, estes sistemas garantem a proteção dos dados ao distribuir toda a informação relevante para a comunicação entre os diversos equipamentos desta "*network*". Outra vantagem notória de não possuir apenas um servidor central reside na *performance* da comunicação entre os diversos elementos do sistema.

A utilização de vários "servidores" para o processamento da comunicação (chegada de pedidos e envio das respetivas respostas) permite aumentar a fluidez do sistema e, assim, evitar possíveis perdas de informações relevantes por sobrecarregamento do servidor.

As redes centralizadas (Figura 2.8 - Direita), por sua vez, concentram todo o poder de armazenamento e controlo do fluxo de informação num único servidor central. Nesta arquitetura, o servidor tem apenas a tarefa de responder aos pedidos dos outros equipamentos (clientes). Este sistema reúne algumas desvantagens a nível de vulnerabilidade do servidor e *performance* na comunicação com os restantes clientes.

A primeira acontece por toda a informação que flui na comunicação estar apenas guardada num servidor central. Numa situação em que o servidor central seja vítima, por exemplo, de um ataque informático, toda a rede que interliga este servidor aos equipamentos clientes pode ficar comprometida. A segunda desvantagem está relacionada com a quantidade de pedidos/respostas que apenas um servidor tem de gerir. Tendo em consideração a elevada quantidade de clientes que podem querer comunicar com o servidor em simultâneo, o elevado fluxo de informação que o servidor tem de gerir pode levar a um sobrecarregamento do sistema. O sobrecarregamento verificado acaba por degradar gradualmente a *performance* do servidor, tornando o serviço obsoleto.

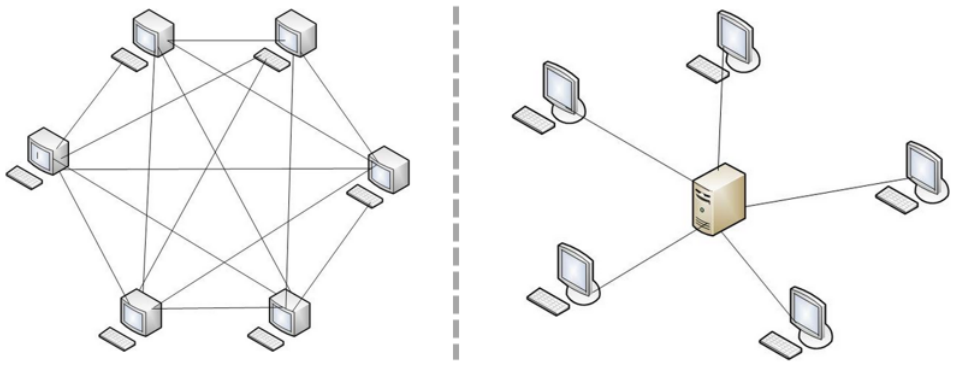


Figura 2.8: Arquitetura Descentralizada (Esquerda) / Arquitetura Centralizada (Direita) [10]. (Adaptada)

Para além destas duas arquiteturas, existe uma terceira, que reúne as vantagens de ambos os sistemas centralizados e descentralizados. Nesta "nova" arquitetura, denominada arquitetura híbrida (Figura 2.9), não existem servidores dedicados a alimentar a

comunicação na rede, mas sim "*super-peers*", que têm a necessidade de atuar como servidores, para alimentar o fluxo de informação entre os diversos equipamentos. Estes "*super-peers*", são equipamentos mais poderosos que os restantes envolvidos na comunicação, que devido à sua elevada *performance*, podem executar o papel de servidores do sistema [10][11].

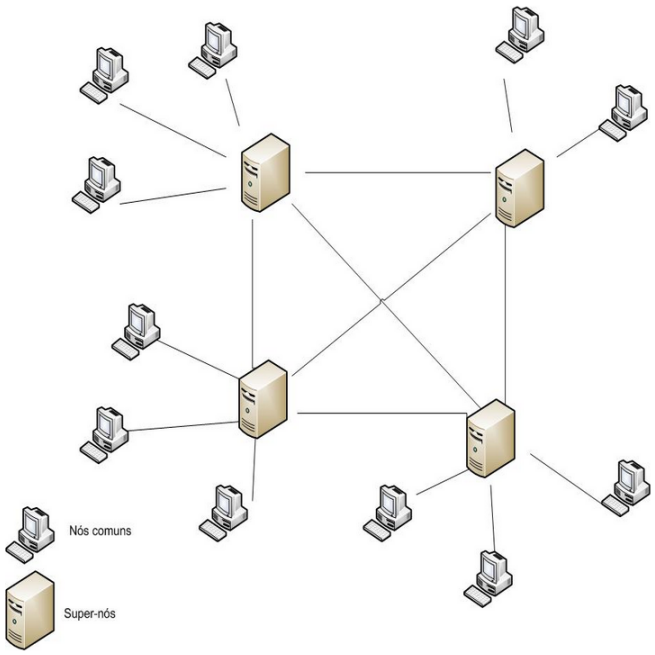


Figura 2.9: Arquitetura Híbrida [10]. (Adaptada)

2.7 Protocolos de Comunicação

Nas tabelas seguintes (Tabela 2.1[12][13] e Tabela 2.2[14]) são apresentadas algumas características relativas aos protocolos GSM (*Global System for Mobile communications*)/GPRS (*General Packet Radio Service*) e Wi-Fi. Estas características permitirão, posteriormente, fazer uma seleção adequada ao pretendido neste sistema.

Tabela 2.1: Características do protocolo GSM/GPRS.

GSM	**GPRS**
• Objetivo de padronizar os telemóveis na Europa; • Permite comunicação por voz e transferência de dados; • Serviço com taxas impostas pela operadora de rede; • *Mobile Station*: Composto por um dispositivo móvel (telemóvel) e um *Smart Card* denominado SIM (*Subscriber Identity Module*). O SIM dá ao utilizador acesso a diferentes serviços e é lido pelo telemóvel.	• Aumenta as taxas de transferência de dados nas redes GSM; • Permite o envio e receção de informação através de uma rede móvel; • Complementa tecnologias de CSD (*Circuit Switched Data*) e SMS (*Short Message Service*); • Permite conexão à Internet sem a necessidade de se estabelecer uma chamada telefónica (*Always On*); • Taxas de transferências na ordem de 171,2 Kbps; • GPRS facilita conexões instantâneas (A informação pode ser enviada ou recebida imediatamente). Não há necessidade de conexões através de *modems*. Utilizadores de GPRS estão "sempre conectados"; • Tem novas aplicações não disponíveis nas redes GSM, devido às limitações de transferência dos CSD's (9,6Kbps) e do tamanho da mensagem SMS (160 caracteres). Permite navegar na WEB e até transferência de dados para automatização de edifícios (controlo e monitorização de equipamentos); • É necessário um telemóvel que suporte GPRS, uma operadora móvel, conhecimento de como enviar e receber informação através do serviço GPRS, entre outros.

Tabela 2.2: Características do protocolo Wi-Fi (802.11).

Wi-Fi
• Ligação entre equipamentos não necessita de cabo; • Permite ligar equipamentos que se encontrem próximos geograficamente; • Transmissão de dados por radiofrequência; • Equipamentos têm de ser compatíveis com esta norma; • Os equipamentos (*Station*) precisam de um aparelho intermediário que lhes forneça acesso à rede (*Access Points*); • Tendo várias *Stations* conectadas a um *Access Point*, obtém-se uma rede (BSS - *Basic Service Set*); • Cada *Access Point* possui uma identificação denominada SSID (*Service Set Identifier*). Isso permite, caso existam muitas redes num mesmo espaço, identificar aquela a que nos pretendemos ligar; • Opera na gama de frequências entre os 2.4 e os 2.4835GHz e tem uma taxa de transmissão de dados de 1 ou 2Mb/s.

2.8 Protocolo TCP/IP

Este protocolo consiste na junção de dois protocolos distintos, o TCP (*Transmission Control Protocol*) e o IP (*Internet Protocol*). O protocolo IP fornece um serviço não confirmado de entrega de mensagens, podendo estas chegar fora de ordem ou não chegar de todo ao destino. Assim, para garantir fiabilidade no envio de informação, é necessário utilizar também o protocolo TCP. Este, por sua vez, fornece um serviço mais fiável, tendo por base alguns serviços disponibilizados pelo IP. Este protocolo cria uma ligação virtual entre os equipamentos de origem e destino, sendo que o TCP tem de estar previamente instalado em ambos os equipamentos. Na transmissão de dados entre os equipamentos recetores e de origem, a receção de dados é sempre confirmada pelo recetor, sendo que, em caso de falha, existe retransmissão automática dos mesmos dados.

O protocolo TCP também permite que dentro do mesmo equipamento existam várias aplicações a comunicarem com o exterior, através da mesma ligação IP. Na receção das mensagens é também garantida a receção de todas as mensagens na ordem desejada, como ilustrado na Figura 2.10 [15].

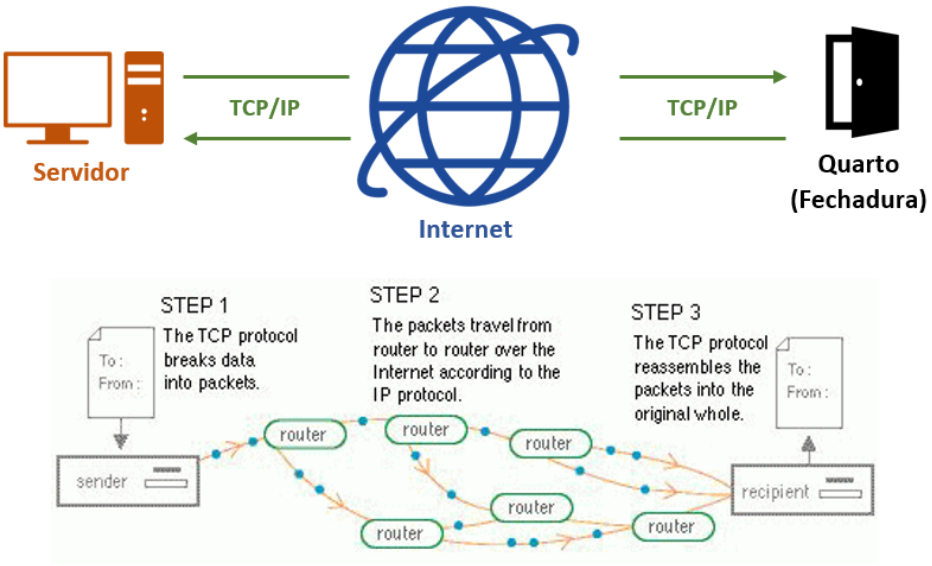


Figura 2.10: Esquema do funcionamento do protocolo TCP/IP [16]. (Adaptada)

2.9 Base de Dados

Uma Base de Dados consiste num repositório de dados organizado sob a forma de tabelas que podem ou não estar relacionadas entre si. Toda a informação em fluxo numa base de dados é gerida por um SGBD (Sistema de Gestão de Base de Dados).

Esses gestores, apesar das suas diferenças comerciais, aceitam pedidos feitos por outros programas, desde que esses pedidos estejam escritos segundo a linguagem SQL (*Structured Query Language*).

Por sua vez, a linguagem SQL permite o envio de uma série de *queries* para consultar, inserir ou alterar os dados inseridos nas respetivas tabelas da base de dados.

Segundo o modelo relacional, uma base de dados não passa de um conjunto de relações (tabelas) relacionadas entre si. É importante referir que cada relacionamento entre relações (tabelas) pode dar origem a uma nova tabela com atributos das relações anteriores. De seguida, serão apresentadas algumas nomenclaturas essenciais no projeto de uma base de dados:

- Cada linha de uma tabela/relação pode ser denominada por **registo**;
- Cada coluna de uma tabela/relação contém **atributos** dos registos;
- O número de atributos de uma tabela/relação tem o nome de **grau da relação**;
- O número de registos de uma tabela/relação é denominado de **cardinalidade** da relação;
- A **chave primária** de uma tabela/relação de uma base de dados relacional consiste num atributo ou conjunto de atributos que representam, de forma biunívoca, um só registo.

No processo de elaboração de uma base de dados, é necessário ter em conta que esta:

- Tem de ter capacidade para guardar todos os dados necessários à empresa;
- Pode ter dados duplicados mas não redundantes;
- Tem de conter o menor número possível de relações;
- Tem de ter as relações normalizadas, de modo a evitar problemas na atualização ou remoção de dados.

Por vezes, ao utilizar apenas uma tabela/relação com todos os dados relativos a uma dada empresa, aparecem dados duplicados e redundantes, que apenas ocupam espaço e não trazem nenhuma informação adicional útil à tabela/relação. Dessa forma, é preferível subdividir essa relação universal em diversas relações, cada uma delas com menor cardinalidade e grau , de maneira a evitar problemas futuros na gestão da base de dados. A esse processo dá-se o nome de normalização da base de dados.

A solução para a normalização de uma base de dados relacional passa pelo uso do método DDF (Diagrama de Dependências Funcionais) entre os atributos de uma relação. Esse método permite, a partir de uma relação universal, gerar um conjunto de sub-relações normalizadas [17].

2.10 Mecanismos para controlo de acessos

Esta secção procura apresentar algumas tecnologias existentes no mercado para controlo de acessos e identificação de determinados utilizadores.

Esta tecnologias, consoante a veracidade da informação introduzida, no momento pretendido, para acesso à entidade protegida, concedem ou negam o acesso ao utilizador. Todo este processo prevê um registo prévio do utilizador nos arquivos do sistema.

2.10.1 Chaves tradicionais

O método mais tradicional de controlo de acessos consiste na utilização de uma simples chave metálica tradicional (Figura 2.11). A evolução das fechaduras e respetivas chaves permite um aumento da segurança do utilizador (dificultando a tentativa de cópia da chave).

Muitas vezes, nos sistemas de controlo de acessos mais recentes, são instaladas fechaduras mecânicas (com chave), juntamente com outras tecnologias mais complexas de identificação do utilizador.

Figura 2.11: Chaves metálicas tradicionais.

2.10.2 Teclado Numérico

Os sistemas com teclado numérico (ou alfanumérico) (Figura 2.12) permitem a introdução de um determinado código para conseguir acesso à entidade pretendida. Existem dois tipos de sistemas com teclado numérico: um com todo o *hardware* e controlo da fechadura na mesma unidade e outro que possui uma unidade paralela de controlo no edifício em que se encontra instalado.

Os sistemas apresentados funcionam de forma semelhante. Após a introdução do código atribuído a determinado utilizador, a fechadura abre ou fecha consoante a veracidade do código introduzido. Por questões de segurança, é conveniente alterar periodicamente os códigos de desbloqueio da fechadura.

Os códigos de acesso são, por vezes, associados aos utilizadores consoante o estatuto que ocupam na empresa em questão. Desta forma, a própria fechadura tem necessidade de registar a informação do utilizador, pertinente ao seu funcionamento.

Este sistema é, normalmente, instalado juntamente com outra tecnologia de controlo de acesso, para aumentar a segurança no acesso a determinada entidade [18].

Figura 2.12: Teclado Alfanumérico [19].

2.10.3 Código de barras

O código de barras consiste numa representação gráfica de determinado valor, ou de uma sequência de dados informativos (sob a forma de dados numéricos ou alfanuméricos), acerca de determinado objeto.

Existem dois tipos principais de códigos de barras: os unidimensionais (1D) e os bidimensionais (2D). Os códigos de barras 1D (mais comuns) são representados segundo um conjunto de barras escuras paralelas de espessura variável, dispostas verticalmente da esquerda para a direita.

Os 2D, por sua vez, ao invés de barras, utilizam quadrados e outros padrões geométricos na sua representação.

A leitura de ambos os códigos pode ser feita com auxílio de leitores óticos, ou até mesmo através de dispositivos com câmara fotográfica. Estes últimos, com recurso a uma aplicação móvel, permitem a obtenção de uma imagem para posterior descodificação.

Um leitor ótico permite a leitura de códigos de barras ao fazer incidir um feixe laser sobre o mesmo. A luz é, então, absorvida nas barras escuras e refletida nas claras. O resultado da reflexão é captado pelo leitor e transformado em impulsos elétricos que, após tratamento, dão origem aos dados pretendidos.

A diversidade de requisitos na identificação levou à criação de normas/simbologias, das quais se destacam a EAN-13 e a UPC [20].

Códigos de barras EAN-13 e UPC

Existem, no mercado, dois grandes tipos de códigos de barras unidimensionais: o EAN-13 (*European Article Number*) e o código UPC (*Universal Product Code*).

O código EAN-13 (Figura 2.13) é utilizado mundialmente (exceto Estados Unidos e Canadá), na identificação de produtos de venda a retalho. Este código é constituído por 13 dígitos, e encontra-se dividido (por ordem) em:

- Filial GS1 (*General Specification*) na qual o código foi originado - Primeiros 3 dígitos;
- Código do Fabricante - 3, 4 ou 5 dígitos;
- Código do Produto - 6, 5 ou 4 dígitos, consoante o número de dígitos do código do fabricante;
- Dígito Verificador - 13º dígito. Este valor é calculado em relação aos restantes 12 dígitos do código (com recurso a um pequeno algoritmo) e permite verificar a validade do código numérico introduzido.

É importante salientar que a soma do número de dígitos dos códigos do produto e do fabricante tem de ser, obrigatoriamente, igual a 9 [21].

Figura 2.13: Código de barras EAN-13.

O código UPC (Figura 2.14), ao contrário do EAN, é utilizado, sobretudo, nos Estados Unidos e Canadá. Este código é constituído por 12 dígitos, com a seguinte estrutura (ordenada):

- Número de Identificação do Fabricante - Primeiros 6 dígitos do código, atribuídos pela UCC (*Uniform Code Council*);
- Identificação do Produto pelo próprio fabricante - 5 dígitos;
- Dígito Verificador - 12º dígito (Mesma função que no código EAN-13).

É fundamental ter em atenção a necessidade de atribuir um código diferente para cada produto [22].

Figura 2.14: Código de barras UPC.

Data Matrix e QR-Codes

A necessidade de transmissão de grandes quantidades de informação levou ao desenvolvimento dos códigos de barras 2D. Os mais relevantes desta família são os conhecidos QR *Codes* (*Quick Response Codes*) e os *Data Matrix*.

Os códigos *Data Matrix* (Figura 2.15) são constituídos por módulos (linhas e colunas) a preto e branco, geralmente apresentados na forma de um quadrado. Quanto maior for a quantidade de informação registada num código deste género, maior também será o seu número de módulos e consequente tamanho. Um *Data Matrix* permite armazenar até cerca de 2300 carateres alfanuméricos. Essa informação pode registar detalhes do componente identificado, como o ID do fabricante, um número de série, entre outros.

Este tipo de códigos é geralmente utilizado na marcação de pequenos componentes, pela sua grande capacidade de armazenamento no menor espaço possível.

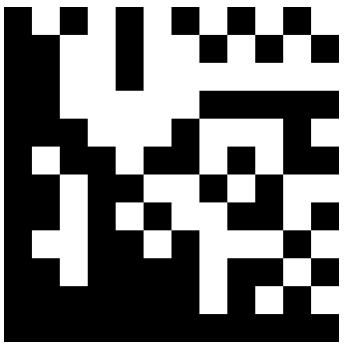


Figura 2.15: Exemplo de código *Data Matrix*.

Os QR *Codes* (Figura 2.16), à semelhança dos *Data Matrix*, são constituídos por um arranjo de módulos pretos dispostos sobre um quadrado com fundo branco. A informação registada no código pode ter formato binário ou alfanumérico.

Para a descodificação da mensagem, são necessários leitores mais potentes que os simples leitores óticos de código de barras. Atualmente, grande parte dos *smartphones* equipados com uma câmara fotográfica permite descodificar este tipo de códigos. Os códigos QR têm sido muito utilizados nas áreas comerciais de *marketing* e entretenimento, para transmissão de informação fácil e rápida aos utilizadores. Para facilitar a sua interpretação pelos respetivos leitores, cada QR *Code* tem um padrão de posição que identifica o tamanho, a direção e o ângulo em que se encontra o código. Por outro lado, este código também contém um padrão de alinhamento que permite ao *scanner* perceber se este se encontra ou não distorcido (por exemplo, se este se encontrar afixado numa superfície cilíndrica). Para além destas características, os QR *Codes* ainda têm associados uma margem de erro que facilita a leitura do código em situações de leitura parcial do mesmo (devido a dano na etiqueta, ou por outro motivo qualquer que não permite a leitura total do código) [23][24][25].

Figura 2.16: Exemplo de código QR.

PDF417

Outro código de barras 2D para armazenamento de grandes quantidades de informação consiste no chamado PDF417 (Figura 2.17). Este código encontra-se dividido por linhas (código linear 1D), podendo ter até 90 linhas. A esta junção de códigos 1D dá-se o nome de "*Stacked Linear Barcode*". A sigla PDF417 significa (por partes):

- **PDF:** *Portable Data File*;
- **4:** Cada padrão no código é constituído por 4 barras e 4 espaços;
- **17:** Cada padrão tem um comprimento total de 17 unidades.

A leitura deste tipo de códigos é realizada com auxílio de um leitor de códigos linear 1D.

As diferenças em relação à leitura de códigos lineares residem na identificação, por parte do leitor, do início e fim de cada "*codeword*", bem como na capacidade do leitor saber a linha do código que se encontra a analisar [26].

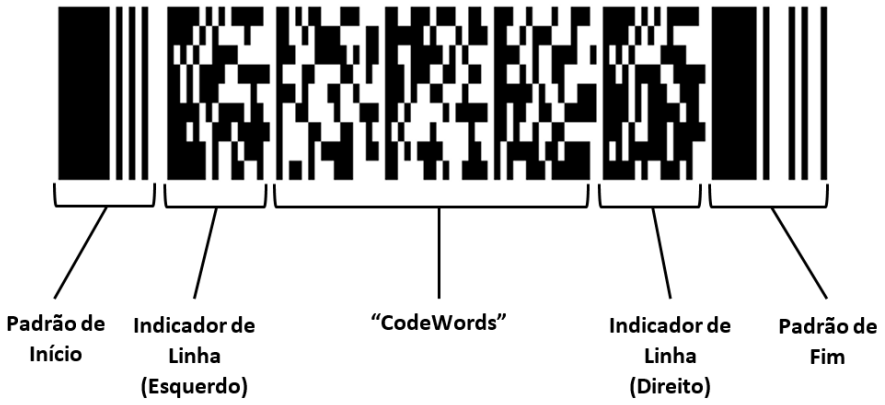


Figura 2.17: Exemplo de código PDF417.

2.10.4 RFID

A tecnologia RFID (*Radio Frequency IDentification*) consiste num método de identificação bastante utilizado na identificação de produtos, veículos e outras aplicações. Para a identificação de determinados elementos, são utilizadas umas etiquetas com informação específica acerca do produto. Devido ao leque de vantagens oferecido pela tecnologia RFID, a sua utilização como alternativa ao código de barras tradicional tem vindo a crescer ao longo destes últimos anos [27].

Tal como nos códigos de barras, a tecnologia RFID também possui um protocolo que permite estruturar a forma como os dados são guardados na etiqueta, bem como a forma como as *tags* (Ver Figura 2.18) e os respetivos leitores comunicam (neste caso, por via aérea). Este protocolo é denominado de EPC (*Electronic Product Code*), e vem facilitar a troca de informação entre diferentes empresas acerca dos produtos comercializados entre si. Como se pode ver pelo nome do protocolo, consegue-se encontrar uma certa semelhança com o UPC usado nos códigos de barras. O EPC é, de certa forma, uma atualização do UPC para as necessidades atuais.

Figura 2.18: Tag RFID Passiva.

Esta tecnologia tem vindo a permitir uma redução de custos a nível empresarial, ao conseguir controlar de forma mais eficiente os níveis de inventário. Isto, para uma empresa de dimensão considerável, pode significar reduções de custos anuais na ordem dos milhões de euros. Apesar de se falar muito da aplicação das RFID no seguimento da vida de um produto, esta tecnologia pode ser aplicada noutras áreas, nomeadamente no controlo de acessos, tema desta dissertação.

A utilização de códigos EPC traz vantagens a nível de rastreabilidade dos produtos lançados no mercado, existindo apenas um e só um para cada produto.

Outro ponto positivo no uso da etiquetas RFID passa pela redução de custos de mão-de-obra na contagem/leitura das mesmas. A leitura das *tags* RFID, em comparação com a leitura de códigos de barras, não impõe a necessidade do leitor se encontrar demasiado próximo, nem alinhado com as etiquetas. Isto favorece a autonomia do sistema, sendo imperativo referir que os sistemas de leitura das *tags* conseguem ler mais que uma *tag* de cada vez.

Por fim, e não menos importante, a tecnologia RFID permite uma atualização em tempo real da informação relativa a determinado item. Essa informação pode permitir ao responsável um controlo mais ativo do estado de determinado produto [28].

Componentes principais do sistema RFID

Um sistema RFID é, por norma, composto por uma antena RFID que permite a comunicação, um *chip* com um código EPC (Ver Figura 2.19) que atribui à *tag* uma identificação única e um equipamento para leitura das *tags*. Este sistema baseia-se na emissão e receção de sinais rádio, que permitem o registo dos dados obtidos na leitura num computador remoto. Este computador também pode, nalguns casos, controlar o leitor de *tags*.

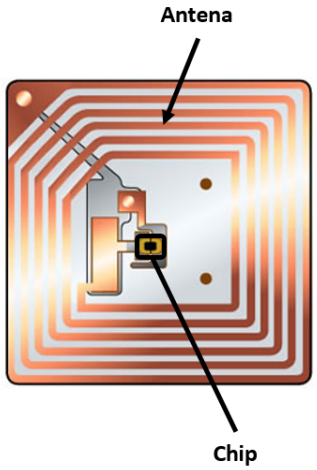


Figura 2.19: Componentes principais de uma *Tag* RFID.

A antena RFID é usada na emissão e receção de ondas eletromagnéticas. Esta é constituída por um filamento metálico e impõe uma frequência de emissão na comunicação com o leitor. A antena, para além das características anteriormente identificadas tem de ter uma impedância compatível com a do *chip*, para otimizar a transferência de energia entre ambas.

O *chip*, como referido anteriormente, contém um código EPC - único para etiqueta - tendo a função de codificar a informação guardada na própria *tag*. Para se poder aceder aos dados guardados no *chip*, é necessário ter presente que o *chip* permite o acesso aos dados de duas formas: apenas como leitura, ou como leitura e escrita. Pode ser também alocada uma memória no *chip* para guardar uma *password* de acesso.

O leitor (Figura 2.20) usado na leitura das *tags* funciona com a emissão e receção de ondas eletromagnéticas, nomeadamente ondas rádio. Em primeiro lugar, o leitor deteta e reconhece o ID da *tag* (fornecido pelo seu fabricante), descodificando posteriormente a informação nela registada.

Figura 2.20: Leitor de *Tags* RFID [29].

As *tags* RFID podem ser classificadas em 3 tipos: as ativas, as passivas e as semi-passivas.

As *tags* ativas (Figura 2.21) diferem das restantes por terem uma bateria que permite alimentar o *chip* e gerar os sinais rádio necessários para a comunicação entre elas e o leitor.

Estas *tags* têm um alcance de leitura bastante superior ao das *tags* passivas, podendo atingir mais de 30 m. A taxa de transferência de dados, neste caso, é bastante rápida, sendo o número de *tags* possíveis de ler em simultâneo consideravelmente elevado.

Estas etiquetas permitem múltiplas leituras e escritas nos *chips*, sendo que a sua vida depende apenas do tempo de vida da sua bateria. Apesar de todas estas características apelativas, estes módulos têm um preço elevado e são demasiado grandes, o que restringe o tipo de aplicações que estes podem servir.

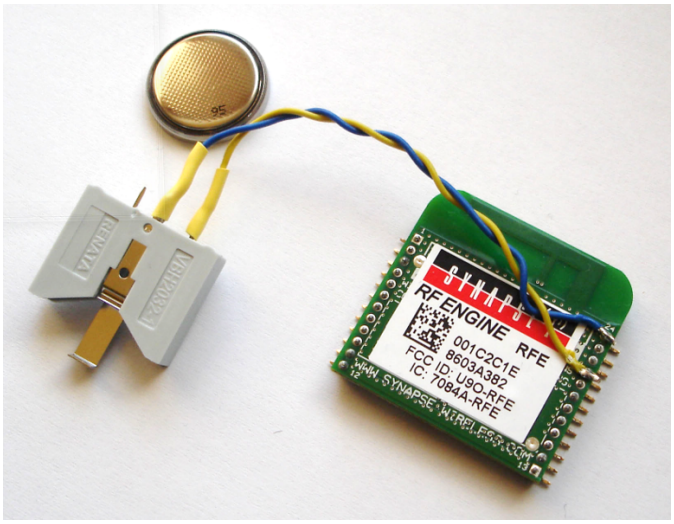


Figura 2.21: *Tag* RFID Ativa [30].

As *tags* passivas, por sua vez, não têm uma bateria embutida, sendo a alimentação do *chip* feita através das ondas rádio emitidas pelo leitor. O alcance de leitura destas etiquetas é de aproximadamente 10 m, notavelmente inferior às ativas. Esta distância de leitura depende, sobretudo, da frequência do sinal emitido. A taxa de transferência de dados, nesta situação, é relativamente baixa, por não se ter uma fonte de alimentação das *tags* suficientemente estável (depende da frequência do sinal). Tal como todas as outras *tags* RFID, podem ser lidas múltiplas *tags* em simultâneo. Os dados guardados no *chip* podem ser lidos várias vezes, apesar de apenas se poder escrever na memória uma vez. Estas *tags* têm a grande vantagem de ter um custo bastante reduzido face às restantes soluções, dimensões bastante reduzidas, assim como um tempo de vida bastante longo.

Finalmente, as *tags* semi-passivas (Figura 2.22) misturam algumas características das *tags* ativas e passivas. Estas têm uma bateria embutida, que apenas serve para alimentar o *chip*. As *tags* continuam a interagir com os leitores através de ondas rádio. Por essa razão, as baterias permanecem inativas grande parte do tempo, aumentando o tempo de vida das respetivas *tags*. O facto de ser usada uma bateria permite aumentar a distância de leitura entre as etiquetas e o leitor, mantendo a fiabilidade dos dados lidos [31].

Figura 2.22: Tag RFID Semi-Passiva [32].

2.10.5 NFC - *Near Field Communication*

A tecnologia NFC (*Near Field Communication*) consiste num método de comunicação sem fios entre dois equipamentos, tendo os seus princípios-base assentes na tecnologia RFID anteriormente referida. Esta tecnologia tem sido um grande marco de revolução no mercado, por ser uma forma de comunicação bastante ecológica (sem fios - OTA (*Over-the-Air*)) e bastante fácil de utilizar (sem necessidade de configurações prévias). É importante salientar que a tecnologia NFC foi implementada no mercado dos equipamentos de comunicação móvel com objetivo de simplificar a vida do utilizador, bem como de garantir a segurança no fluxo de informação entre diversos equipamentos.

As potencialidades da utilização desta tecnologia já são visíveis nalgumas aplicações comuns no quotidiano de qualquer indivíduo. Alguns exemplos dessas aplicações são: terminais de pagamento multibanco, validação de bilhetes de metro, identificação e controlo de acessos, entre outros (Ver Figura 2.23).

Figura 2.23: Exemplos de utilização da NFC: 1-Pagamentos Multibanco [33]; 2-Bilhetes de Metro [34]; 3-Controlo de Acessos [35]; 4-Troca de Ficheiros [36]. (Adaptada)

O princípio de funcionamento da tecnologia NFC assemelha-se, em grande parte, ao funcionamento de *tags RFID* passivas. Algumas características que ilustram as diferenças/melhorias desta tecnologia relativamente à sua "antecessora" RFID são:

- Comunicação entre equipamentos de curto alcance;
- Apenas são utilizadas *tags* passivas (na leitura e escrita de informação na *tag*);
- A troca de dados é bastante segura devido ao curto alcance de comunicação;
- A compatibilidade existente entre os diferentes tipos de NFC permitiu agilizar a ligação entre dois dispositivos, sendo apenas necessários aproximá-los para iniciar a transferência de dados.

Sabendo que a tecnologia RFID permite comunicações de longo alcance, este método é considerado propício à interceção de informação por entidade alheia. Por exemplo, as *tags* RFID passivas (que não têm uma fonte de energia associada para permitir o início da comunicação) conseguem ter um alcance de leitura na orla dos 10 m (Figura 2.24). As inconveniências apresentadas levaram ao desenvolvimento da tecnologia NFC.

Figura 2.24: Distância de Comunicação NFC [37][38] . (Adaptada)

A transferência de dados entre dois equipamentos NFC acontece com a aproximação/contacto entre os dois dispositivos equipados com as respetivas *tags*. A comunicação entre os dois equipamentos é feita no sentido do equipamento ativo para o equipamento passivo. O *chip* do equipamento ativo cria um pequeno campo eletromagnético que induz corrente na *tag* NFC passiva do equipamento de destino. Nesse instante, o equipamento ativo envia um pedido de ligação ao equipamento passivo. O papel da *tag* NFC passiva assenta na receção do pedido e posterior resposta ao equipamento ativo com a informação nela registada.

O equipamento que inicia a comunicação tem de ser, obrigatoriamente, um equipamento ativo. Isto acontece porque este tipo de equipamento tem uma fonte de alimentação que permite sustentar a comunicação entre os dois equipamentos. O equipamento recetor, por sua vez, tanto pode ser um ativo (com fonte de alimentação) como um passivo (sem fonte de alimentação)(Ver Figura 2.25).

Na eventualidade deste ser um ativo, a energia utilizada na resposta ao pedido reside na energia da fonte de alimentação do próprio equipamento. Caso o recetor seja um passivo, a resposta ao pedido é conseguida com a utilização do campo eletromagnético gerado pelo iniciador da comunicação [39].

Figura 2.25: Tipos de comunicação NFC.

Em termos de modos operacionais, a comunicação NFC consegue operar em 3 modos diferentes:

1. **Leitura/escrita:** Estes modos permitem a troca de informação entre um equipamento ativo e uma *tag* NFC. A leitura de informação contida numa *tag* NFC passiva (e não só) pode ser feita por qualquer equipamento ativo (*smartphone* ou leitor NFC). A escrita (registo de informação na *tag*), por sua vez, apenas pode ser realizada por um equipamento ativo;

2. ***Peer to peer*:** Neste modo, cada equipamento presente na comunicação tem a sua própria fonte de alimentação, ou seja, cada um deles utiliza o seu próprio campo eletromagnético para o envio de informação. Nesta comunicação, é esperado um diálogo entre equipamentos do tipo *half-duplex*, ou seja, enquanto um equipamento envia um determinado pedido, o outro limita-se apenas a escutar;

3. ***Card emulation*:** Esta situação prevê a utilização do equipamento ativo como um *smart card*, dando-lhe assim, o poder de interagir com um leitor NFC. Um equipamento ativo (neste caso, pode utilizar-se o exemplo do *smartphone*) tem a capacidade de armazenar a informação relativa a diferentes *contactless smart cards*. O modo de emulação permite selecionar, consoante a aplicação necessária no momento (cartão multibanco, cartão de acesso a um quarto, entre outros), qual o *smart card* a utilizar. Alguns exemplos das aplicações possíveis para este modo são os terminais de pagamento multibanco, o serviço de bilheteira para metros, controlo de acessos em infraestruturas, entre outros.

A tecnologia NFC utiliza, para a transferência de dados, uma frequência de 13.56 MHz, igual à utilizada na comunicação RFID. Atualmente, são conseguidas velocidades de transferência de dados bastante consideráveis, conseguindo-se atingir velocidades na ordem dos 424 kbps. Quando os dois equipamentos se encontrarem emparelhados, inicia-se uma aplicação no dispositivo, cujo objetivo é gerir a passagem de informação [40].

A tecnologia NFC assume nos seus pressupostos, que apenas 3 tipos de equipamentos podem comunicar com NFC:

- **Equipamento ativo:** Este equipamento consiste naquele que inicia a comunicação. Atualmente grande parte dos *smartphones* tem integrada uma *tag* NFC

que lhes concede a capacidade de funcionar como equipamentos ativos de uma comunicação deste tipo, entre dois equipamentos. A integração da tecnologia NFC nos equipamentos de comunicação móvel tem aumentado substancialmente o seu potencial de utilização;

- **Leitor NFC:** O leitor NFC é um equipamento que permite a transferência de dados entre dois terminais NFC (o leitor e outro). Os terminais multibanco que permitem pagamento por NFC são um exemplo destes leitores (Figura 2.26);
- ***Tag* NFC passiva:** A *tag* NFC passiva consiste numa *tag* RFID com menor alcance de interação e que carece de uma fonte de alimentação própria (Figura 2.26).

Figura 2.26: Leitor NFC (Esquerda); Tag NFC (Direita).

Tipos de codificação

A tecnologia NFC recorre a dois tipos de codificação para a transmissão de dados entre equipamentos: a codificação *Modified Miller* e a codificação *Manchester*. Como se pode verificar na Tabela 2.3, para as diferentes velocidades de transferência de dados apresentadas, a codificação mais utilizada por *tags* ativas e passivas consiste na codificação *Manchester*.

Tabela 2.3: Tabela de codificações NFC - **ASK**: Amplitude Shift Keying

Taxa de Dados (Kbps)	Equipamento Ativo	Equipamento Passivo
106	*Modified Miller*, 100%, ASK	*Manchester*, 10%, ASK
212	*Manchester*, 10%, ASK	*Manchester*, 10%, ASK
424	*Manchester*, 10%, ASK	*Manchester*, 10%, ASK

Codificação *Modified Miller*

Este tipo de codificação define quais os *bits* a 0 e a 1 consoante a posição do pulso ao longo de um "*bit period*". Tendo em consideração a Figura 2.27, um "*bit period*" encontra-se dividido em 4 segmentos. Um *bit* a 1 corresponde a dois valores "*high*", seguido de um valor "*low*" e outro "*high*".

Por sua vez, um *bit* a 0 pode ter duas representações possíveis, dependendo dos seus *bits* precedentes.

Na eventualidade do *bit* anterior ser 0, o primeiro valor do *bit* a 0 corresponde a um primeiro valor "*low*" seguido de três "*high*". Caso o *bit* anterior ao bit a 0 seja um bit a 1, os quatro valores do bit a 0 encontram-se a "*high*".

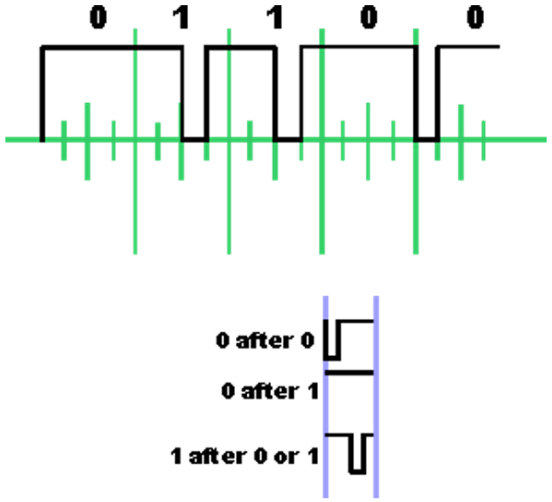


Figura 2.27: Codificação *Modified Miller* [41]. (Adaptada)

Codificação *Manchester*

A codificação *Manchester*, como referido anteriormente, consiste na codificação mais utilizada nas comunicações NFC. Este método espera a divisão de cada "*bit period*" em dois segmentos, para, assim, analisar o tipo de transição verificada nesse ponto central.

Na eventualidade de se verificar uma transição de "*low*" para "*high*", o *bit* correspondente é o *bit* 0. Caso a transição seja do tipo "*high*" para "*low*", o *bit* toma o valor 1 [42] - (Ver Figura 2.28).

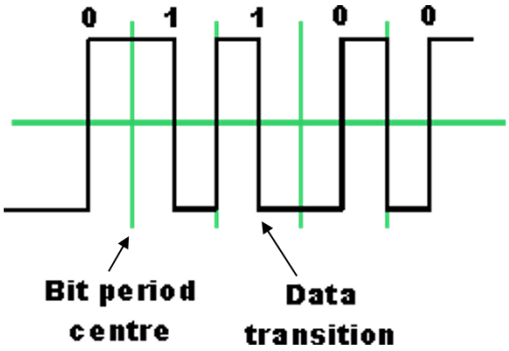


Figura 2.28: Codificação *Manchester* [41]. (Adaptada)

Conceitos inseridos na tecnologia NFC

- ***Secure element* (SE):** SE consiste numa plataforma segura, capaz de armazenar aplicações e dados confidenciais segundo normas de segurança pré-estabelecidas. Este SE pode tomar forma de um *chip* com memória interna e funções capazes de encriptar ou desencriptar dados envidados/recebidos.

  No momento pretendido para a utilização da tecnologia NFC, o controlador NFC presente no equipamento entra em modo de emulação, dando seguimento do pedido para o SE. O controlador NFC toma, neste caso, o papel de intermediário entre o que é pedido e a resposta pretendida.

  Posteriormente, o SE entra em ação e cede os dados necessários para a aplicação pretendida [43].

- **Ativo:** Um dispositivo ativo consiste num equipamento que tem uma fonte de energia interna integrada. Essa fonte de energia permite criar um campo eletromagnético necessário para iniciar a comunicação com outro equipamento.

- **Passivo:** Um dispositivo passivo, por outro lado, não contém uma fonte de energia interna integrada. Ele usa, neste caso, o campo eletromagnético gerado pelo ativo, para poder responder ao pedido que recebeu.

- ***Smart Card*:** Um *smart card* consiste num cartão com um circuito elétrico integrado e memória integrada para o posterior armazenamento de dados. Existem atualmente 3 tipos de *smart cards*:

  - ***Contact smart cards*:** Estes cartões recebem a energia necessária para a sua leitura através de contacto físico entre o cartão e o leitor.
  - ***Contactless smart cards*:** Este tipo de cartões recebe energia do campo eletromagnético gerado pelo leitor, para a leitura dos dados registados na sua memória. Após o cartão ter armazenado energia suficiente, este pode responder ao pedido que o equipamento ativo lhe fez.

    Neste caso, os cartões apenas conseguem comunicar quando os intervenientes na comunicação estão suficientemente próximos um do outro. Uma das principais razões para esta proximidade prende-se na segurança dos dados trans-

mitidos entre os dois equipamentos, sendo que outra consiste na quantidade de energia transferida entre o equipamento ativo e passivo.

- **Hybrid smart cards:** Mistura os dois conceitos anteriores.

Os *smart cards* são cartões que não contêm uma fonte de energia interna associada. A energia necessária para a leitura dos dados neles registados é fornecida por um equipamento exterior (por exemplo, um leitor).

Como se pode verificar através de uma análise superficial, os *contactless smart cards* são os que mais se aproximam à tecnologia em estudo nesta secção. Os *smart cards*, por sua vez, também se podem dividir em três tipos:

- ***Close coupling smart cards*:** Estes cartões são utilizados para situações em que a distância entre os equipamentos, na leitura, ronda os 1 cm.
- ***Proximity coupling smart cards*:** Este tipo de cartão é o mais comum no mercado, sendo que consegue operar a distâncias na ordem dos 10 cm, a uma frequência de 13.56 MHz.
- ***Vicinity coupling smart cards*:** Os *vicinity smart cards* são cartões que se assemelham aos usados em controlo de acessos. Estes cartões operam a distâncias até 1 m, a uma frequência de 13.56 MHz.

Como foi referido anteriormente, os *proximity smart cards* são os mais comuns no mercado, por estarem associados a uma maior diversidade de aplicações. Estes cartões, por sua vez, também se encontram divididos em 3 tipos diferentes, segundo a sua popularidade:

- **MIFARE:** Estes cartões são os mais comuns no mercado, representando cerca de 80% dos *contactless smart cards*. Estes cartões foram desenvolvidos por uma empresa pertencente ao grupo Philips.
- **Calypso:** Os cartões Calypso foram desenvolvidos por um conjunto de companhias europeias ligadas à transação de mercadorias. Estes cartões têm a função de permitir um maior seguimento dos produtos ao longo do seu ciclo de vida, assim como facilitar transações de mercadorias entre diferentes associações, até chegar ao consumidor final.
- **FeliCa:** Os FeliCa foram desenvolvidos pela Sony com o propósito de serem utilizados em cartões bancários. Este tipo de cartões nunca chegou a ser considerado norma ISO/IEC [39].

2.10.6 Biometria

A Biometria corresponde a uma tecnologia que permite a medição e análise de algumas características físicas e comportamentais do corpo humano, tais como impressões digitais, íris, veias, padrões de voz e escrita, entre outros. Essa informação é posteriormente processada, para fins de autenticação do utilizador.

Este tipo de sistema de controlo de acessos é cada vez mais comum no mundo dos sistemas de segurança comerciais. Os dispositivos biométricos são principalmente constituídos por:

- Aparelho de leitura;
- *Software* que converte a informação digitalizada para formato digital e compara os pontos comuns;
- Base de dados que armazena dados biométricos para comparação.

De forma a evitar um possível roubo de identidade, é garantida a encriptação de toda a informação biométrica recolhida no momento de registo do utilizador [44].

Apesar da complexidade deste tipo de sistemas de segurança, as etapas necessárias na verificação da permissão que determinado utilizador tem ao tentar aceder a determinado espaço são semelhantes às necessárias noutros tipos de sistemas deste género [45].

- **Inscrição:** Esta etapa existe com o intuito de registar o utilizador na primeira vez que entra em contacto com o dispositivo biométrico. Para além de dispensar alguma da sua informação pessoal (Nome, NIF, Morada, etc.), são também registados alguns dados biométricos do utilizador (registo de voz, *scan* da íris, impressão digital, etc) para futura comparação aquando da tentativa de acesso.
- **Armazenamento:** O processo de armazenamento consiste no registo da informação adquirida na etapa anterior numa base de dados (ou algo semelhante), para futura comparação numa tentativa de acesso à entidade desejada. Numa tentativa de reduzir o espaço ocupado por uma imagem ou gravação de voz, toda a informação recolhida no registo é convertida num código, num gráfico, ou até mesmo num *smart card*.
- **Comparação:** Numa posterior tentativa de acesso, o sistema recorre à informação previamente registada na base de dados, para comparação com a informação lida no momento pelo dispositivo biométrico. Tendo em consideração o resultado da comparação entre a informação introduzida e registada, o utilizador poderá ter ou não acesso à entidade pretendida.

A instalação de um sistema de segurança deste tipo garante um nível de segurança muito grande, comparativamente aos sistemas de controlo de acessos referidos nas secções anteriores. Esta garantia de segurança é conseguida face à dificuldade de obtenção da informação biométrica de determinado utilizador.

As tecnologias para registo e leitura de informação biométrica apresentadas nesta secção, são (por ordem):

1. Escrita;
2. Impressão Digital;
3. Voz;
4. Íris;
5. Veias.

Escrita

A identificação de utilizadores através da escrita consiste num método bastante mais complexo do que parece. Este sistema biométrico procura examinar o ato de escrever, e não apenas a forma de cada letra de uma assinatura. Para isso, é utilizado um grande número de sensores, que têm por objetivo analisar a pressão, a velocidade e o ritmo da escrita. Os sensores utilizados podem ser canetas (detetar o ângulo, pressão e direção da escrita), ou até as próprias superfícies de escrita. Na comparação com os dados armazenados, são também utilizados dados, como a sequência de caracteres introduzidos (acentuação, etc.).

O *software* utilizado na comparação da informação introduzida com a registada, traduz a informação em gráficos que permitem reconhecer o utilizador no momento de acesso à entidade pretendida. Este *software* também permite fazer pequenas alterações à informação registada na base de dados, com um algoritmo que deteta pequenas variações na escrita do utilizador (Ver Figura 2.29).

Figura 2.29: Sistema de reconhecimento do utilizador pela escrita [45]. (Adaptada)

Impressão digital e Geometria da Mão

Este sistema permite a identificação de determinado utilizador a partir da geometria da sua mão, ou até mesmo da(s) sua(s) impressão(ões) digital(ais). Tendo em consideração a possibilidade de existir mais do que uma pessoa com uma geometria de mão semelhante, a identificação através de uma impressão digital é sempre considerada mais fiável. Por essa razão, os leitores de geometria da mão são maioritariamente utilizados para autenticação de utilizadores, mas não para sua identificação.

O registo da informação é conseguido com auxílio de uma câmara digital, juntamente com uma fonte luminosa. Para auxílio na leitura, os leitores possuem uma superfície lisa com pinos que delimitam a zona de colocação da mão e dos dedos do utilizador. As imagens obtidas são utilizadas para determinar o comprimento, a largura, a espessura e a curvatura dos dedos e da respetiva mão.

Toda a informação obtida neste processo de leitura é posteriormente convertida num

formato numérico, para subsequente comparação com informação registada na base de dados.

Este sistema não é considerado dos mais seguros no mercado, devido a possíveis problemas encontrados na leitura da mão de determinado utilizador, como:

- Semelhanças entre as mãos de dois ou mais utilizadores distintos;
- Deformações fisiológicas causadas por doenças ou acidentes;
- Alterações na geometria da mão, relacionadas com um aumento/diminuição de peso.

Algumas soluções biométricas deste género permitem uma atualização constante da informação, consoante pequenas alterações da geometria da mão ao longo do tempo (Ver Figura 2.30).

Figura 2.30: Sistema de reconhecimento do utilizador pela geometria da mão [46]. (Adaptada)

Os leitores de impressão digital, tal como referido anteriormente, permitem uma identificação mais eficaz e assertiva de um indivíduo. A impressão digital consiste no desenho formado por pequenas irregularidades nas pontas do dedos que se combinam de tal forma a não existirem duas iguais no mundo. A leitura destas impressões pode ser feita de duas formas: através de um *scanner* ótico, ou através de um *scanner* capacitivo.

O primeiro consiste num dispositivo que utiliza, da mesma forma que nalgumas câmaras digitais, um sensor semicondutor para captação de imagens, denominado CCD (*Charge Couples Device*). O processo de leitura da impressão digital inicia com a colocação do dedo num prato de vidro e com a subsequente fotografia tirada pela câmara CCD. O leitor tem, por norma, uma fonte luminosa, que existe com o intuito de iluminar as irregularidades presentes na impressão digital. O sensor CCD, por sua vez, gera um negativo da imagem, em que as zonas escuras representam as zonas com maior intensidade de luz refletida (irregularidades), e onde as zonas mais claras representam as zonas de menor intensidade de luz refletida (cavidades entre as irregularidades).

Por sua vez, os *scanners* capacitivos, à semelhança dos anteriores, permitem gerar imagens com as irregularidades e respetivas cavidades constituintes da impressão digital. Este sensor, ao invés de uma fonte luminosa, utiliza corrente elétrica para leitura da impressão digital.

Estes sistemas biométricos de controlo de acessos permitem o registo de uma ou várias impressões digitais, para identificação de um qualquer utilizador. Isto acontece como forma de precaução na eventualidade de acontecer algum acidente que altere a geometria da impressão digital de um dos dedos registados (Ver Figura 2.31).

Figura 2.31: Sistema de reconhecimento do utilizador pela impressão digital [47]. (Adaptada)

Voz

Alguns sistemas biométricos de controlo de acesso funcionam através do reconhecimento da voz do utilizador que pretende aceder a uma dada entidade. Estes sistemas concedem acesso após a comparação do espectrograma registado no momento da tentativa com os registados numa base de dados remota. Um espectrograma consiste num gráfico que contém no seu eixo vertical a frequência do som e no eixo horizontal o tempo decorrido

desde o inicio da gravação. Após comparação da informação retida nos dois gráficos, pode ser autorizado ou negado o acesso do utilizador à entidade pretendida, consoante a coincidência verificada na sua sobreposição.

Alguns destes sistemas apresentam falhas de segurança, por não se encontrarem devidamente preparados para distinguir uma gravação de um telemóvel (ou outro dispositivo do género) de um registo de voz real (Ver Figura 2.32).

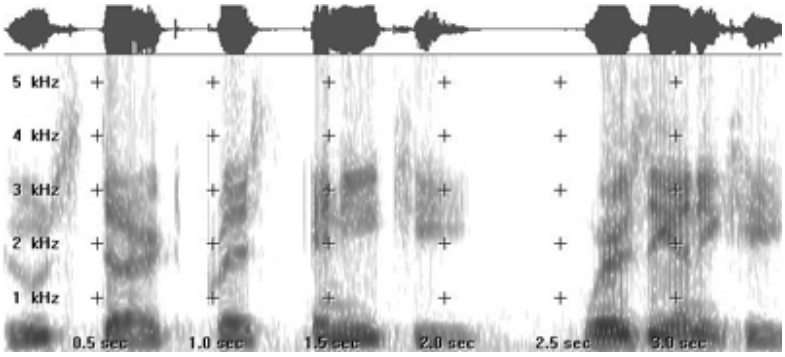


Figura 2.32: Sistema de reconhecimento através da voz do utilizador [45]. (Adaptada)

Íris

Os sistemas de leitura e reconhecimento da íris funcionam de forma semelhante aos leitores óticos de impressão digital. Esta semelhança deve-se ao facto de ambos os sistemas utilizarem um sensor CCD. A captura de imagens é conseguida com o auxílio de uma câmara digital (com sensor CCD), luz infravermelha e luz visível. Estes dois espectros de luz permitem a obtenção de imagens com uma grande qualidade e contraste, para fácil separação entre a íris e a pupila.

Este sistema apenas requer algum cuidado no posicionamento do utilizador para garantir uma leitura correta e eficaz. Após a leitura e respetiva separação da íris, o *software* utilizado converte a imagem (com um conjunto relativamente elevado de pontos de referência) em código. Esse código é posteriormente utilizado para comparação com informação registada na base de dados, garantindo acesso na eventualidade de existir correspondência.

A identificação de um utilizador através da íris é considerada dos métodos mais seguros, sendo implementada em ambientes com requisitos de segurança muito elevados. Esta segurança deve-se à unicidade da íris, bem como à consistência da sua forma ao longo dos anos (mesmo após operação ao olho) (Ver Figura 2.33).

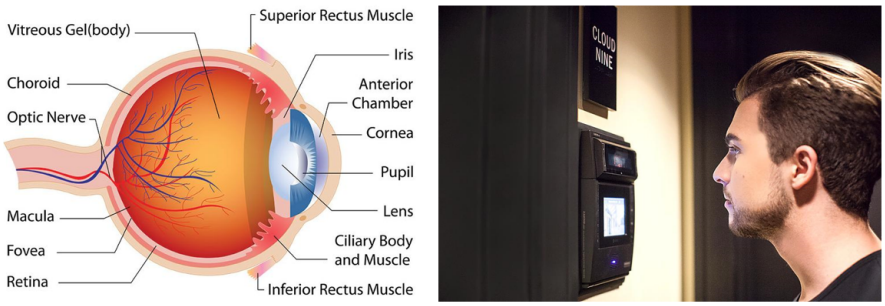


Figura 2.33: Sistema de reconhecimento através da íris do utilizador [48][49]. (Adaptada)

Veias

Um dos sistemas biométricos de identificação mais seguro reside num sistema de identificação através da disposição das veias. Esta característica, à semelhança da íris e da impressão digital, é única de pessoa para pessoa, diferindo até entre membros semelhantes (por exemplo, duas mãos). A leitura deste sistema é feita com recurso a luz infravermelha e, por norma, é feita a identificação através de um braço do utilizador.

Este sistema permite a obtenção da geometria das veias através da incidência de luz infravermelha no braço do utilizador. A hemoglobina presente no sangue absorve a luz infravermelha, dando origem a uma imagem do braço com as veias marcadas num tom mais escuro.

À semelhança dos restantes dispositivos biométricos, o *software* deste sistema converte a informação da localização das veias e respetiva geometria num modelo que é posteriormente comparado com a informação registada na base de dados da solução.

Na eventualidade da informação registada no momento da tentativa de acesso corresponder à informação registada na base de dados, será concedido acesso ao utilizador em questão (Ver Figura 2.34).

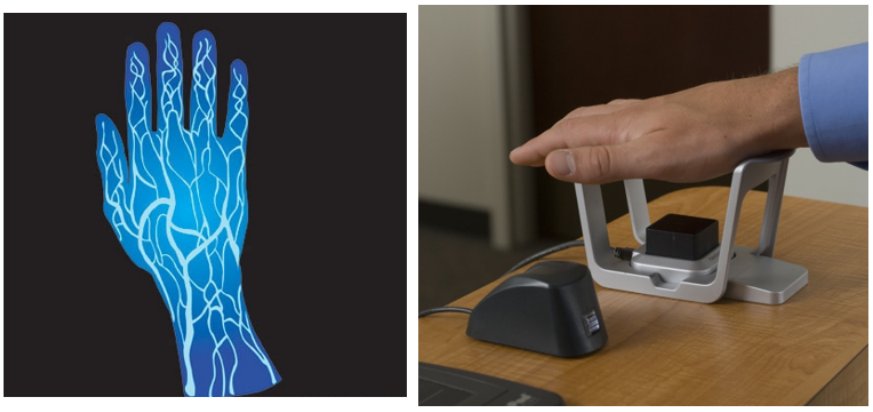


Figura 2.34: Sistema de reconhecimento através das veias da mão do utilizador [50][45]. (Adaptada)

Face

A tecnologia biométrica de reconhecimento facial permite o reconhecimento de determinado utilizador através do mapeamento da estrutura óssea do seu rosto (distância entre os olhos, nariz, boca e orelhas). Esse mapeamento é feito com auxílio de uma imagem tirada no momento de tentativa de acesso. A imagem é posteriormente tratada e convertida num modelo numérico, sendo consequentemente comparada com os rostos registados na base de dados.

Na verificação da identidade do utilizador, os termos comparados consistem na forma do rosto, na sua estrutura e proporção, na distância entre os olhos, nariz, boca e queixo, contorno superior das órbitas, lados da boca, localização do nariz e dos olhos, entre outros.

Depois de inscrito na base de dados do sistema, o utilizador tira um conjunto de imagens em diversos ângulos e com diferentes expressões faciais. Isto acontece como medida preventiva, na tentativa de tentar utilizar uma imagem de um indivíduo registado como forma de acesso à entidade alheia[44] (Ver Figura 2.35).

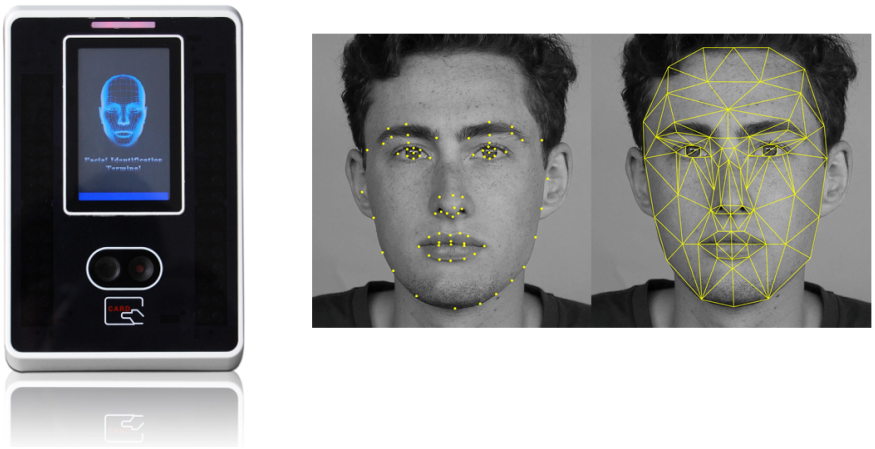


Figura 2.35: Sistema de reconhecimento através da face do utilizador [51][52]. (Adaptada)

2.10.7 Soluções existentes

Esta dissertação tem por objetivo apresentar um sistema revolucionário que permite o aproveitamento de alguns aspetos positivos de soluções existentes no mercado, patentes do INPI (Instituto Nacional de Propriedade Industrial), ou até mesmo de alguns projetos e dissertações encontrados no decorrer do desenvolvimento desta solução. Para além do aproveitamento das vantagens apresentadas, espera-se o acréscimo de algumas funcionalidades de relevo, que marcam a diferença entre o produto proposto e as soluções já existentes.

Os documentos utilizados para posterior análise e melhoria dos sistemas propostos são:

- Duas dissertações de mestrado;
- Duas patentes;

- Algumas soluções de controlo de acessos da marca "Chaves do Areeiro".

Na primeira dissertação apresentada, datada de 2014, o autor propôs uma solução de controlo de acessos, que tem por meta a simplificação do processo de identificação dos utilizadores no acesso a alojamentos hoteleiros. O dispositivo de identificação, nesta situação, consiste na tecnologia RFID, que apenas necessita de uma *tag* e de um leitor para a sua posterior descodificação. A comunicação entre a porta do alojamento e a base de dados do sistema é conseguida com auxílio de um equipamento de comunicação "ZigBee" (XBee), que permite a troca de informação através do uso de comandos AT.

Para além do sistema físico de controlo de acessos, é fundamental o desenvolvimento de uma interface que possibilite a gestão de toda a informação do sistema. Esta interface reside num aplicativo que concede acesso personalizado à informação pretendida, tendo em conta o *Username*, a *Password*, a entidade e o estatuto de cada utilizador. As credenciais submetidas permitem diferenciar o tipo de informação apresentada ao utilizador, visto que o seu papel no sistema poder ser de cariz administrativo ou utilitário (cliente) [53].

Na segunda dissertação, datada de 2015, o autor apresenta uma solução que se encontra repartida em três módulos principais:

- Base de dados do sistema;
- Plataforma de reservas;
- Fechadura "inteligente" do alojamento pretendido.

Toda a informação necessária ao bom funcionamento da plataforma de reservas e da fechadura encontra-se registada na base de dados do sistema. A plataforma de reservas, como o nome indica, tem a função de permitir ao cliente efetuar a reserva do espaço pretendido entre as datas desejadas. Após conclusão da reserva, é assegurado o envio de um email com o código de acesso ao espaço, bem como toda a informação necessária ao suposto acesso ao alojamento.

Cada cliente, no momento pretendido de acesso ao alojamento, apenas tem de estabelecer uma ligação Wi-Fi com o micro-controlador ESP embutido na fechadura e digitar o código fornecido no email da reserva. Todos os passos de ligação ao ESP são também apresentados no email da reserva.

Após confirmação dos dados introduzidos com os dados registados na base de dados para a reserva em vigor, é, então, apresentada uma página que permite o controlo da fechadura através da ativação de saídas digitais do ESP [6].

As duas patentes estudadas nesta dissertação têm por base o mesmo sistema de identificação, que permite um acesso personalizado aos utilizadores envolvidos. Tendo em consideração a falta de informação apresentada nos pedidos de patente, apenas se pode concluir que o sistema de controlo de acessos funciona segundo a tecnologia RFID. Para o funcionamento da solução, apenas é necessária a aproximação de uma *tag* específica ao leitor embutido numa porta. Para além da tecnologia de identificação utilizada, também é referido que cada módulo embutido na fechadura tem a capacidade de comunicar com o servidor central da solução, através do protocolo TCP/IP. Essa valência permite uma maior autonomia do sistema [54][55].

A marca "Chaves do Areeiro" disponibiliza no seu catálogo algumas soluções para controlo de acessos na indústria hoteleira, das quais se destaca o sistema "Kaba Oracode".

Esta solução, segundo a informação disponibilizada no site da empresa, apresenta as seguintes especificações:

- 100% autónoma;
- Gestão de autorizações simples, que funcionam por códigos de utilizador;
- Hierarquia até 8 níveis de utilizadores (para facilitar o controlo de hóspedes, pessoal de limpeza, entre outros);
- Não necessita de ligações cabladas.

Ao não necessitar de ligações cabladas, este sistema torna-se bastante simples de instalar, o que favorece a redução de custos na sua implementação [56].

Outra solução da marca "Chaves do Areeiro" reside num sistema de controlo de acessos denominado "Kaba Modelo E-790". Este modelo funciona segundo a tecnologia RFID, e assegura a privacidade e segurança dos seu utilizadores. Este sistema permite o cancelamento automático das *tags* na data de *check-out* prevista para uma dada reserva [57]. Todas as soluções da Chaves do Areeiro contêm dispositivos manuais de abertura em caso de falha de energia (Ver Figura 2.36).

Figura 2.36: Kaba Oracode (Esquerda); Kaba Modelo E-790 (Direita).

Apesar das inúmeras vantagens dos sistemas acima apresentados, as lacunas presentes no seu desenvolvimento e funcionamento podem afetar a decisão do comprador na sua escolha entre as diversas opções "em cima da mesa". Em comparação com o sistema proposto nesta dissertação, as soluções acima apresentadas apresentam algumas falhas das quais:

1. **Dissertação 2014 - José Carmo**

   - Falta de uma aplicação/página WEB para efetuar a reserva, pagamento e respetiva confirmação;
   - A utilização da tecnologia RFID como método de controlo de acessos não permite a automatização total do sistema, por requerer sempre uma pessoa para a programação e entrega das *tags* aos clientes.

2. **Dissertação 2015 - David Cardoso**

   - A falta de um método para pagamento o automático da reserva compromete a ideia de automatização total do sistema;
   - A utilização da tecnologia RFID como método de controlo de acessos não permite a automatização total do sistema, por requerer sempre uma pessoa para a programação e entrega das *tags* aos clientes;
   - Para acesso ao alojamento é obrigatório o cliente ter acesso a um equipamento com capacidade de acesso a um browser WEB e capacidade de se conectar à rede do ESP.

3. **Patentes**

   - Falta de um sistema de reservas automático, que permite o pagamento e respetiva receção da confirmação;
   - A utilização da tecnologia RFID como método de controlo de acessos não permite a automatização total do sistema, por requerer sempre uma pessoa para a programação e entrega das *tags* aos clientes.

4. **Soluções comerciais - Chaves do Areeiro**

   - A "Kaba Oracode" funciona *offline*, ou seja, não permite uma atualização automática das reservas em vigor e do código de acessos a elas associado (Não tem capacidade de se conectar à Internet para atualização constante, segundo informação disponível na base de dados do sistema);
   - A "Kaba Modelo E-790A" utiliza a tecnologia RFID como método de controlo de acessos. Sendo assim, esta solução não permite a automatização total do sistema, por requerer sempre uma pessoa para a programação e entrega das *tags* aos clientes;
   - Existe a incerteza da existência de um sistema de reservas automático que permite o pagamento imediato da reserva e receção da sua respetiva confirmação.

2.11 Tecnologia Escolhida para suporte à Identificação do Utilizador

Um dos principais objetivos da solução proposta neste documento assenta na automatização total do sistema de controlo de acessos e de registo de reservas.

Para isso, é necessário garantir que a tecnologia de suporte à identificação escolhida não utilize forçosamente a ajuda de mão humana para o registo da informação do utilizador. Sendo assim, todos os sistemas biométricos apresentados são imediatamente descartados ao exigirem um registo prévio da informação pertinente para a identificação do cliente no momento de acesso ao quarto.

Uma das condições a garantir consiste na simplicidade de utilização do sistema, juntamente com o custo do equipamento necessário para o bom funcionamento do sistema de identificação do utilizador.

Na tabela seguinte (Tabela 2.4) são apresentadas algumas vantagens e desvantagens notórias de cada mecanismo de controlo de acessos apresentado na secção anterior (Secção 2.10):

Tabela 2.4: Algumas características dos mecanismos de controlo de acessos apresentados.

Tecnologia	**Vantagem**	**Desvantagem**
Teclado Numérico	• Apenas requer a memorização do código de acesso (Não necessita de dispositivo de suporte para armazenamento o código); • Implementação simples e com custo reduzido.	É relativamente lento, comparativamente aos restantes, por precisar do esforço de digitação do utilizador.
Código de Barras	Acesso à entidade pretendida relativamente rápido e com esforço reduzido por parte do utilizador.	• É necessário ter equipamento de suporte para armazenar código (papel, cartão ou telemóvel); • Equipamentos de leitura com preço elevado, aquando da sua implementação em grande escala; • Fácil captura da informação.

RFID	Acesso à entidade pretendida relativamente rápido e com esforço reduzido por parte do utilizador.	• Recurso a objeto físico para retenção do código (Requer o envio do objeto ao utilizador, ou até mesmo alguém sempre disponível para fazer a entrega no *check-in*); • Fácil captura da informação; • Equipamentos de leitura com preço elevado, aquando da sua implementação em grande escala.
NFC	• Acesso à entidade pretendida relativamente rápido e com esforço reduzido por parte do utilizador; • Para acesso à entidade pretendida, o utilizador apenas necessita de ter o seu telemóvel consigo; • Maior segurança da informação registada no equipamento devido ao curto alcance de comunicação.	• Nem todos os *smartphones* disponíveis no mercado têm NFC implementado; • Para registo da informação necessária no *smartphone* é necessária a emulação do *chip* NFC no local da estadia, para acesso à entidade pretendida (pessoa dedicada para o efeito).
Biometria	Método bastante seguro que identifica univocamente cada indivíduo.	• Método bastante caro de implementar; • Método invasivo para o utilizador; • Registo da informação biométrica requer a presença antecipada do indivíduo no estabelecimento.

As únicas soluções que apresentam vantagens, tendo em consideração os objetivos apontados, são os códigos de barras e o teclado numérico.

A tecnologia NFC, apesar de ter um potencial de implementação bastante interessante, tem a desvantagem da pré-configuração da *tag* para emulação do controlo de acessos.

As restantes aplicações têm desvantagens a nível de custos de implementação, autonomia do sistema de registo, assim como dos equipamentos terceiros necessários para acesso ao alojamento.

Existem muitos sistemas de identificação do utilizador implementados em unidades hoteleiras que permitem o acesso com auxílio a *tags* RFID. Esse sistema, apesar das suas vantagens, parece carecer de autonomia no seu funcionamento, por ser sempre necessário o registo do código na *tag* e na entrega da *tag* ao utilizador respetivo.

Os códigos de barras, apesar de oferecerem uma certa autonomia ao sistema de identificação do utilizador (dada a possibilidade de gerar um código automático no momento da reserva), têm um custo de implementação em grande escala relativamente elevado e necessitam sempre de um suporte físico ou digital para armazenamento do código.

A necessidade de envio de determinado objeto ao utilizador com o código de acesso pode levar ao incumprimento do objetivo de automatização total da solução.

Tendo em consideração toda a informação apresentada anteriormente, a solução mais adequada para a autenticação do utilizador encontra-se, possivelmente, na identificação através de um teclado numérico e respetivo código de acesso.

Este mecanismo permite, através de uma rotina de processamento automático, o envio do código de acesso ao utilizador, após a reserva e o respetivo pagamento. Isto favorece a ideia de automatização total do sistema, evitando a ação humana para interação com o cliente.

Capítulo 3

Solução Proposta

Este capítulo tem o objetivo de dar a conhecer a solução proposta, assim como a ordem de trabalhos seguida no seu desenvolvimento. Para caracterizar o modelo apresentado, seguiu-se a lógica do modelo Cliente/Servidor, sendo a solução dividida consoante a interação existente entre estes.

Para isto, serão apresentados um conjunto de pré-requisitos necessários ao bom funcionamento do produto apresentado.

3.1 Solução Proposta

A solução apresentada neste capítulo tem por objetivo atender às necessidades de automatização do processo de reservas e controlo de acessos, na indústria hoteleira. Esta solução procura permitir a comunicação, através da rede Internet, entre os diversos constituintes deste sistema de reservas e controlo de acessos, apresentados na Figura 3.1.

Atualmente, um dos grandes problemas verificados na indústria hoteleira assenta nos custos de funcionamento de uma receção. A necessidade de atendimento em contínuo (24/24 horas) impõe a existência de, pelo menos, 3 turnos diários, ou seja, em termos salariais, 3 ordenados por mês. Na eventualidade de existir uma solução que permita às instalações hoteleiras prescindir dos serviços de uma receção, as vantagens seriam notórias, não só na redução de custos, mas também na redução de tempos de *check-in*. A redução dos tempos de *check-in* está diretamente associada ao conforto de utilização do serviço oferecido ao cliente, visto permitir o acesso direto ao quarto, sem ter a necessidade prévia de passar pela receção.

A solução apresentada neste capítulo tem por objetivo apresentar alguns aspetos necessários à resolução dos problemas expostos anteriormente, de forma a futuramente, se obter uma solução eficiente e vantajosa de implementar nas instalações pretendidas. Visto o pretendido ser a obtenção de um sistema funcional e totalmente autónomo, a necessidade de desenvolver uma plataforma WEB com toda a informação dos quartos, e com a possibilidade de reservar um desses alojamentos é imprescindível. A plataforma, para além das funções expostas anteriormente, contribui para o aumento do conforto do cliente, ao permitir efetuar a reserva e o seu respetivo pagamento (através do "PayPal"), sem necessidade de se deslocar previamente ao estabelecimento onde reside o alojamento pretendido.

Dessa forma, a plataforma WEB consiste no elo de ligação entre o cliente e a base de

dados do sistema, registando, assim, todos os dados relativos ao cliente e à sua respetiva reserva. Também é esperado que a plataforma ofereça ao proprietário do(s) alojamento(s) a capacidade de monitorização das reservas e da atividade do cliente durante a estadia, assim como o controlo de todos os dados disponibilizados na plataforma.

No que toca ao controlo de acessos, é necessário desenvolver uma fechadura que tenha a capacidade de saber qual a reserva que está em vigor e, por conseguinte, saber qual a chave de acesso que permite ao cliente usufruir do alojamento. Essas características contribuem para uma maior autonomia do sistema, sendo o próprio cliente a fazer o *check-in* no momento pretendido para usufruto do quarto. A fechadura tem, por essa razão, de ser capaz de comunicar com a base dados do sistema, de modo a adquirir os dados necessários ao seu funcionamento.

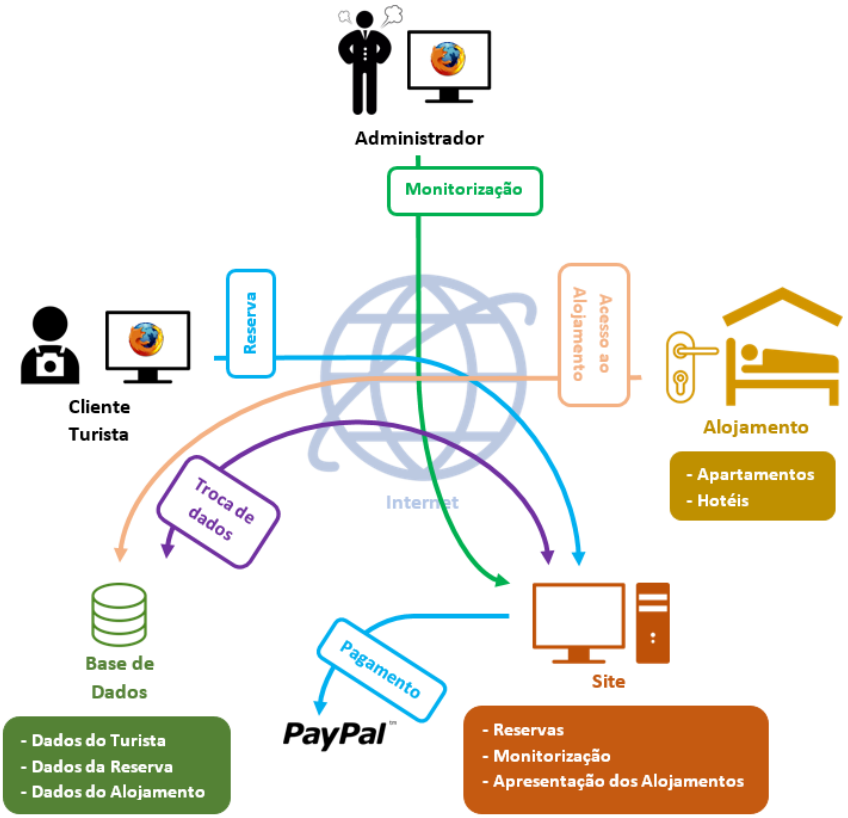


Figura 3.1: Esquema da Solução Proposta.

3.2 Reserva

De forma a poder efetuar a reserva do espaço pretendido, é necessário o cliente ter acesso, através de um computador ou outro dispositivo móvel com acesso à Internet, a um *browser WEB* que permita aceder à plataforma WEB do sistema de reservas.

No decorrer do processo de reserva, é pedido ao cliente alguma da sua informação pessoal que o identifique, para efeitos de registo, sendo essa informação posteriormente armazenada numa tabela específica da base de dados do sistema. Para além dessa infor-

mação, também são registados todos os dados relativos à reserva em questão, como: o quarto pretendido, as datas de *check-in* e *check-out*, o código de acesso, o valor a pagar e respetiva confirmação de pagamento - dados esses posteriormente associados ao nome do cliente que fez o pedido de reserva.

No fim do processo, após a chegada da confirmação de pagamento, é enviado um email ao cliente com toda a informação relativa à reserva efetuada, juntamente com o código de acesso ao alojamento pretendido. Na Figura 3.2, pode-se observar o esquema de comunicação entre o cliente, a plataforma WEB (*Site*) e a base de dados do sistema, sendo, posteriormente, especificado na Figura 3.3 o diagrama de interações entre esses 3 elementos.

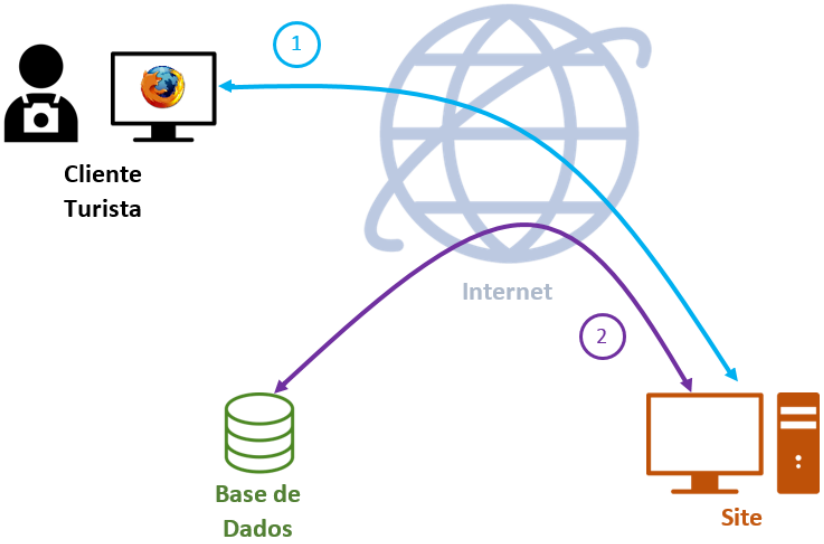


Figura 3.2: Esquema da comunicação para a reserva.

Para além de registar os dados dos clientes e das reservas, a base de dados também tem o papel de ceder toda a informação necessária à plataforma sobre os quartos, ou até mesmo sobre as reservas efetuadas, para efeito de monitorização. Sendo assim, essa comunicação permite atualizar a informação despendida aos clientes na plataforma WEB, mostrando apenas os quartos disponíveis nas alturas desejadas, juntamente com as suas respetivas especificações.

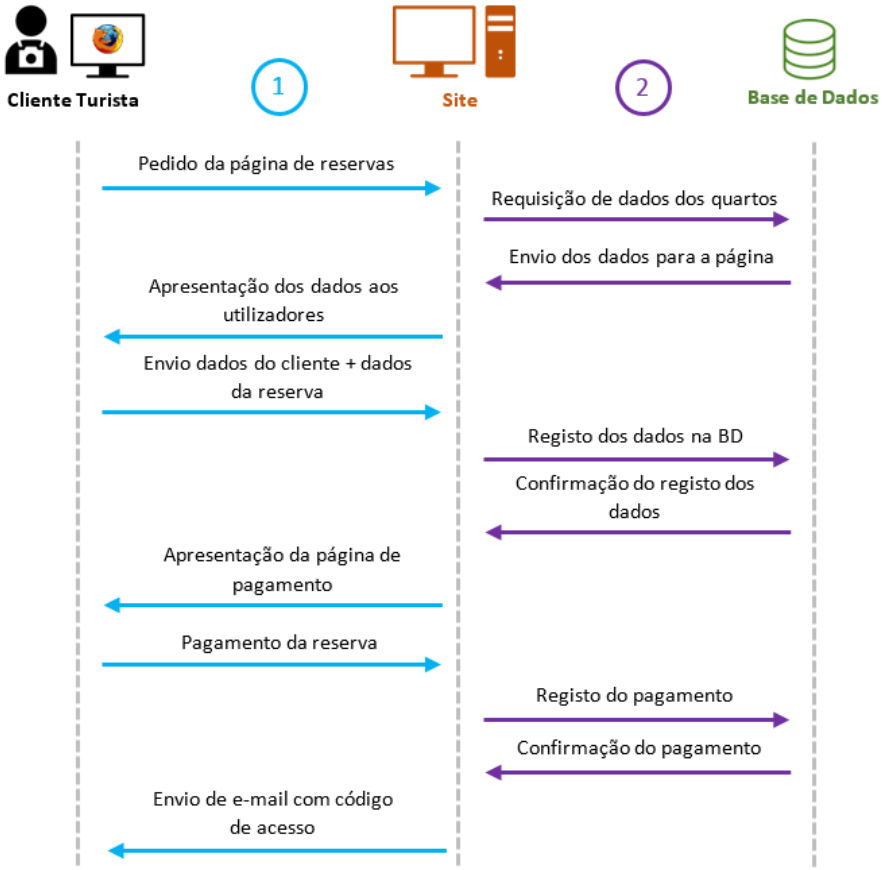


Figura 3.3: Diagrama de Interação entre os 3 intervenientes do processo de reserva.

3.3 Acessos ao Alojamento

O acesso ao alojamento é baseado na interação entre o cliente e a fechadura do sistema. A fechadura desta solução, como referido anteriormente, tem de ser "inteligente" o suficiente para conseguir autorizar ou negar o acesso aos clientes, consoante as datas de *check-in* e *check-out* escolhidas no momento da reserva. Para isso, tendo por base a Figura 3.4, a fechadura tem de conseguir comunicar com uma Base de Dados, de forma a conseguir acesso aos dados pretendidos. A necessidade de globalização da ideia proposta, impõe a utilização da rede Internet como meio de transporte para o fluxo de dados trocados entre os diversos intervenientes do sistema.

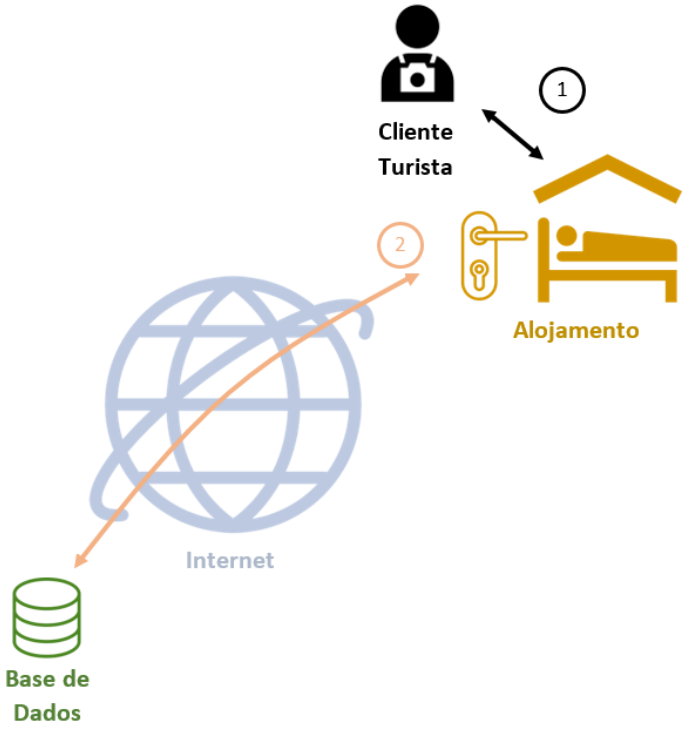


Figura 3.4: Esquema da Comunicação para o Acesso ao alojamento.

A escolha do método utilizado na identificação de cada utilizador assenta naquele que permite dar à solução proposta a maior autonomia possível, a um preço relativamente acessível. Tendo em consideração os aspetos apresentados, uma fechadura aliada de um teclado alfanumérico aparenta ser a solução que mais se enquadra nos objetivos previstos. No momento de tentativa de acesso a um dado alojamento, a fechadura tem de conseguir interpretar os dados digitados no teclado, de modo a controlar a abertura e o fecho do trinco da porta. Em adição às funcionalidades expostas, esta permite também controlar as entradas e saídas do quarto, sendo esse registo feito com o auxílio de sensores magnéticos, comuns para este tipo de utilização. Esta última função está enquadrada no serviço de monitorização, por parte do administrador do espaço, oferecido pelo sistema.

Um dos cuidados tidos em consideração na implementação da solução proposta, para evitar despesas extra a nível da alteração de infraestruturas existentes, assenta na dimensão do produto final. A necessidade de garantir uma solução com dimensões reduzidas, leva à utilização de um microcontrolador para processamento dos dados necessários ao funcionamento da fechadura. Esta tecnologia, para além de ter um grande custo-benefício, garante uma comunicação suficientemente estável entre a fechadura e os restantes intervenientes do sistema.

As necessidades de comunicação da solução proposta neste capítulo não permitem a ligação cablada entre os diversos constituintes do sistema, sendo, por essa razão, imperativo o uso de redes sem fios. Para este tipo de comunicação, é fulcral a presença, a nível intermédio, de um ou vários *Access Points*. Esses equipamentos, também conhecidos por *routers*, têm por função difundir as mensagens enviadas pelo cliente através da rede Internet.

No sistema proposto, é esperado que cada fechadura tenha a capacidade de comunicar com uma base de dados, por forma a adquirir o código de acesso ao quarto e as datas de *check-in* e *check-out* relativas à reserva em questão. Esta automatização do processo permite uma redução da interação administrador/proprietário-cliente, facilitando, assim, todo o processo, desde a reserva ao *check-in* no local.

No momento desejado para acesso ao espaço alugado, caso a data atual esteja compreendida entre as datas limites da reserva, o código digitado será comparado com o código registado na base de dados e poderá ser concedido ou negado o acesso ao alojamento. Atualmente, as soluções existentes no mercado são implementadas com um código de acesso predefinido que pode ou não ser alterado consoante o tipo de equipamento, ou os custos externos que essa mudança implica.

Na Figura 3.5 está apresentado um diagrama de interações entre os 3 elementos presentes no processo de acesso ao alojamento, que permite compreender melhor o fluxo de informação necessário para um bom funcionamento da fechadura do sistema.

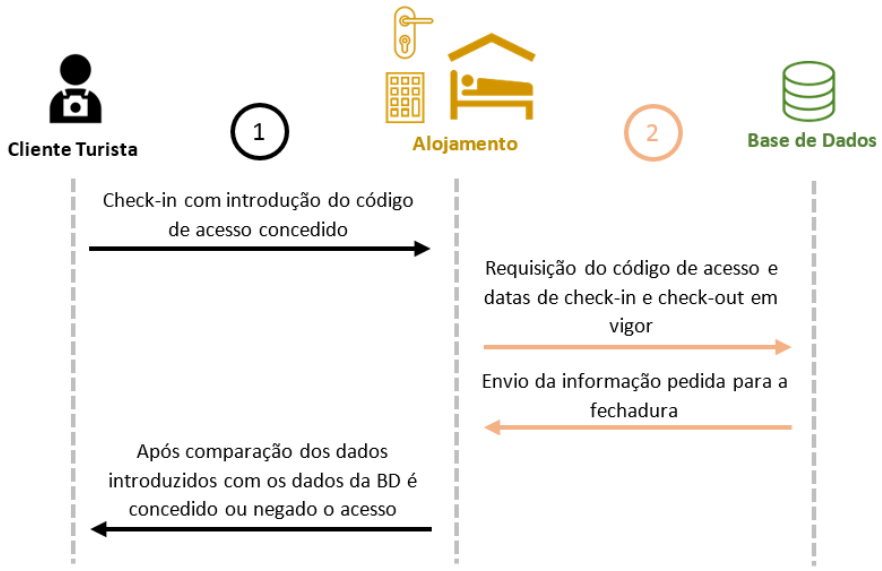


Figura 3.5: Diagrama de Interação entre os 3 intervenientes do processo de acesso ao alojamento.

3.4 Monitorização

O serviço de auditoria oferecido pela plataforma de reservas (*site*) tem por objetivo a monitorização das reservas efetuadas, assim como o controlo sobre a informação disponibilizada para cada alojamento. Para ter acesso às funcionalidades deste serviço, o administrador do sistema tem de efetuar o seu *login* na plataforma. Por forma a garantir a diversidade entre o *login* do(s) cliente(s) e do(s) administrador(es), as credenciais de identificação do segundo são registadas diretamente na base de dados da solução, antes da sua instalação nos espaços pretendidos.

Na página de monitorização, apresentada após confirmação dos dados de *login* introduzidos, encontra-se toda a informação relativa às reservas em vigor, aos quartos disponíveis na plataforma (para posterior consulta dos clientes), e às faturas emitidas após a receção do pagamento da reserva.

Esta funcionalidade, ao encontrar-se embutida na plataforma de reservas, permite o seu acesso através de qualquer *browser* WEB, em qualquer parte do mundo, dando assim uma ideia de globalização do conceito proposto. Na Figura 3.6 é possível observar um diagrama representativo dos diversos intervenientes presentes no acesso, por parte do administrador dos alojamentos, ao serviço de monitorização da solução apresentada neste capítulo.

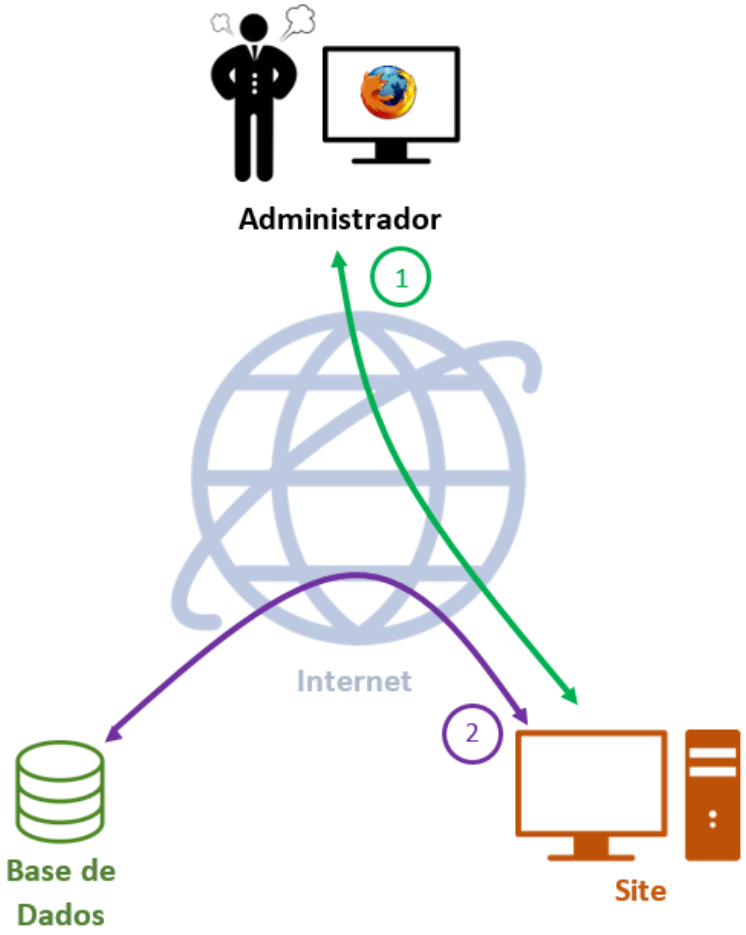


Figura 3.6: Esquema da Comunicação para a Monitorização por parte do Administrador.

Tendo agora em consideração a Figura 3.7, é possível visualizar que no processo de acesso à página de monitorização estão presentes 3 elementos principais: o Administrador, a Plataforma de reservas (*Site*) e a Base de dados do sistema. Todo o processo visível na interação do administrador com a plataforma de reservas, impõe uma comunicação em *background* entre a plataforma e a base de dados da solução. A base de dados consiste, na realidade, no "cérebro" deste serviço, ao conter toda a informação necessária para o correto funcionamento deste sistema de reservas. A página de monitorização permite

alterar/remover alguma da informação presente na base de dados, controlando, assim, as reservas pendentes, assim como toda a informação disponibilizada sobre os quartos existentes.

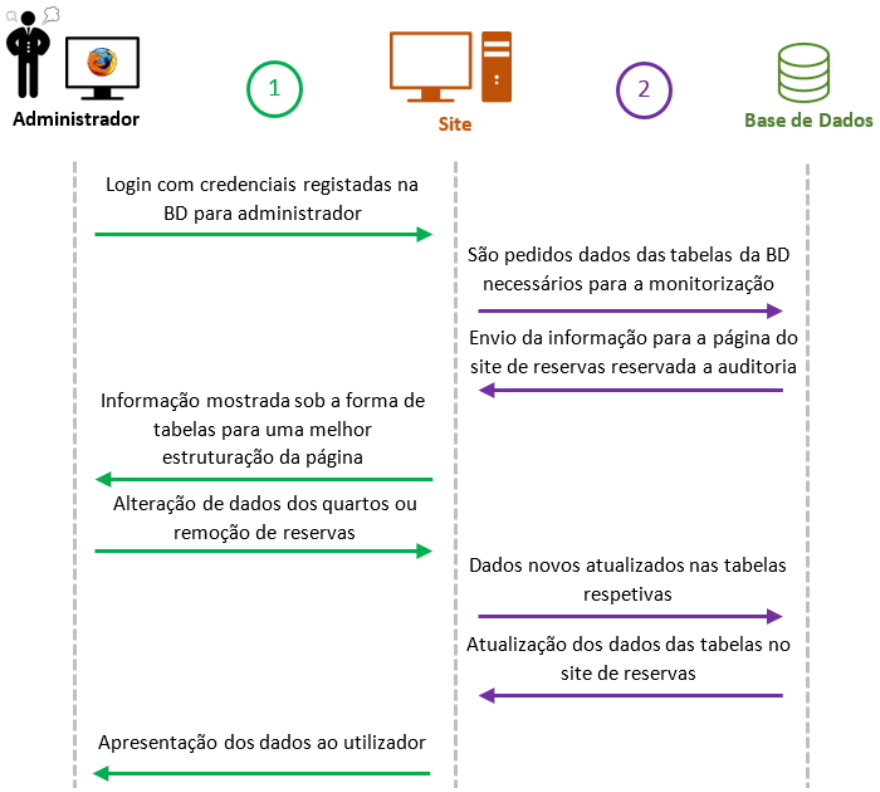


Figura 3.7: Diagrama de Interação entre os 3 intervenientes do processo de Monitorização.

Capítulo 4

Implementação da Solução

Este capítulo pretende dar a conhecer o conjunto de etapas necessárias à implementação da solução proposta. O processo de implementação do sistema encontra-se dividido em 3 partes essenciais:

- Solução implementada: Esta secção apresenta detalhadamente a solução desenvolvida, juntamente com alguns critérios tomados na escolha da arquitetura do sistema e no tipo de comunicação da fechadura com outros equipamentos;
- *Software*: A secção de *software* procura apresentar toda a parte relativa ao desenvolvimento da plataforma de reservas e programação do microcontrolador da fechadura do alojamento;
- *Hardware*: Esta secção pretende apresentar os diversos componentes integrantes do sistema em estudo, bem como aprofundar alguns aspetos técnicos necessários ao seu bom funcionamento.

4.1 Solução Implementada

A solução apresentada, como sugerido no capítulo anterior, assenta em três grandes funcionalidades: a reserva do alojamento pretendido, a monitorização dos espaços por parte do administrador do sistema, assim como o acesso ao espaço reservado.

Desta forma, o sistema proposto divide-se em 5 intervenientes principais: o proprietário dos alojamentos, o cliente que pretende usufruir dos espaços disponíveis, o próprio alojamento, o servidor da plataforma de reservas e a base de dados da solução. Na Figura 4.1, encontra-se ilustrado o esquema final da solução implementada, com os tipos de comunicação entre os vários intervenientes e todos os equipamentos terceiros necessários para o bom funcionamento do sistema de controlo de acessos e registo de reservas apresentado neste documento.

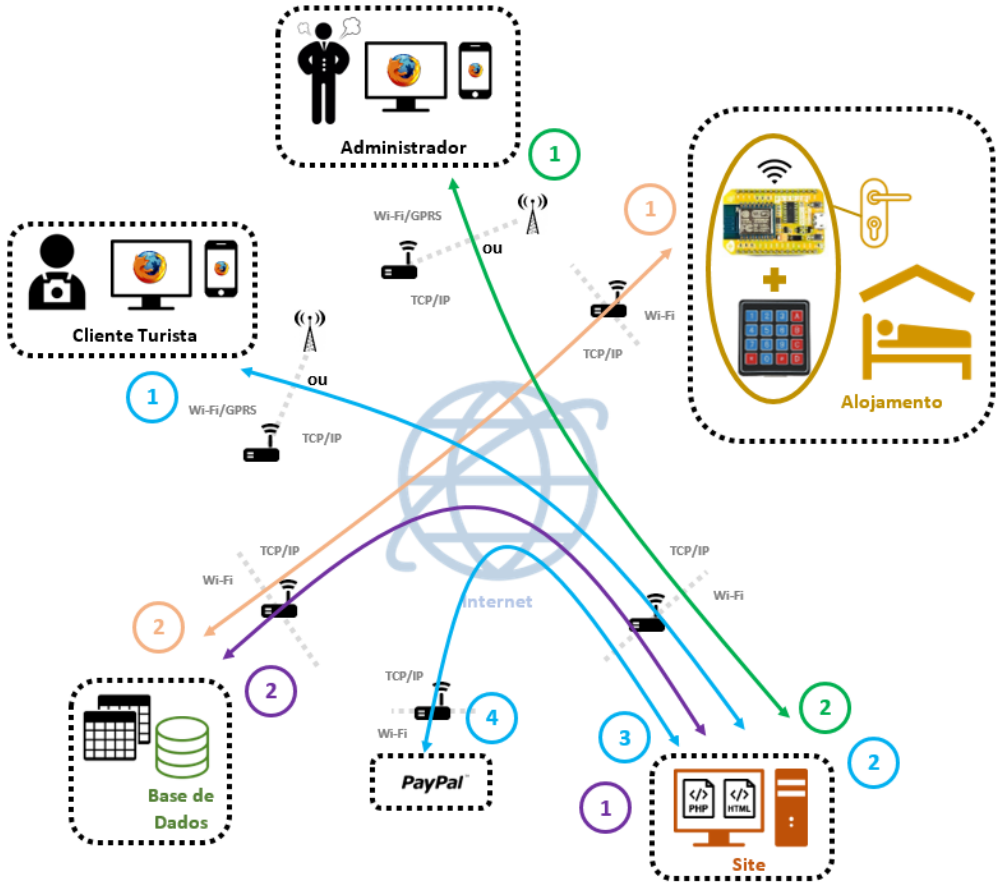


Figura 4.1: Esquema da Solução Implementada.

Segundo o esquema proposto na Figura 4.1, tanto a reserva do alojamento pretendido (pelo cliente), como a monitorização dos espaços (pelo administrador do sistema) têm em comum dois intervenientes: a plataforma de reservas (*site*) e a base de dados da solução. É importante referir que esta última também se encontra presente no acesso ao espaço reservado, sendo, por isso, considerada como "cérebro" do sistema proposto.

Um dos pressupostos esperados na concretização da solução proposta nesta dissertação assenta na automatização do processo de reservas e controlo de acessos num determinado alojamento. Em primeiro lugar, a automatização do processo de reservas assenta no desenvolvimento de uma plataforma de reservas que permite ao cliente efetuar a reserva do alojamento pretendido para as datas de *check-in* e *check-out* desejadas. Esta plataforma também permite, em "cooperação" com a plataforma de pagamentos online "PayPal", efetuar o pagamento das reservas efetuadas, aumentando o conforto do cliente e do administrador dos espaços, ao evitar possíveis entraves no pagamento e na sua respetiva confirmação.

Em segundo lugar, o desenvolvimento de uma fechadura "inteligente" capaz de gerir as reservas em vigor nas datas de tentativa de acesso ao alojamento também contribui para uma maior autonomia do sistema, não sendo, assim, necessário, a cada novo *check-in*, "ensinar" manualmente à fechadura qual o código de acesso que permite fazer usufruto do espaço pretendido.

Para além destas vantagens notórias para o cliente, o administrador dos espaços disponibilizados também pode usufruir da plataforma de reservas, sendo-lhe concedido o poder de monitorizar as reservas efetuadas, bem como controlar toda a informação disponibilizada na própria plataforma. Para aceder a este serviço, o administrador tem apenas de fazer o *login* na plataforma, sendo-lhe posteriormente apresentado um conjunto de tabelas com a informação relativa às reservas em vigor, às faturas emitidas para cada reserva e aos dados da base de dados relativos a cada alojamento.

É também importante realçar que, para o caso em estudo, tendo em consideração a necessidade de acesso ao espaço reservado de forma autónoma, existindo a nível intermédio uma troca de informação entre a fechadura e a base de dados do sistema, é fundamental a adoção de um protocolo que permita a comunicação entre a fechadura e outros periféricos que permitam o acesso à rede Internet. Neste caso, foram estudados dois microcontroladores distintos, que permitem, indiretamente, o acesso à rede Internet segundo diferentes protocolos de comunicação:

- SIM900 - Protocolo GSM/GPRS;
- ESP8266 - Protocolo Wi-Fi 802.11;

Nas secções seguintes, serão aprofundados alguns tópicos relacionados com o modelo cliente-servidor implementado, com a arquitetura de sistema escolhida para esta solução e com os protocolos de comunicação necessários para uma comunicação eficaz entre os diversos equipamentos envolvidos nesta *network*.

4.1.1 Modelo Cliente/Servidor

Uma solução para controlo de acessos tem de ter em conta 4 passos essenciais, com o objetivo de autorizar ou negar o acesso a determinado utilizador. Como foi referido no Capitulo 2, o acesso a determinada entidade passa por um conjunto de etapas:

- **Identificação do utilizador**: Inicialmente, antes de poder aceder ao espaço pretendido, o utilizador necessita de estar registado nos arquivos do sistema. Para isso, é necessário que este ceda alguma da sua informação pessoal que o distinga dos restantes utilizadores. Toda essa informação é posteriormente armazenada num servidor remoto de acesso público que garante a sua segurança, fiabilidade e disponibilidade imediata, caso necessário;
- **Autenticação dos dados introduzidos**: Após estar concluída a identificação do utilizador, segue-se a reserva do espaço pretendido. Este processo termina com o pagamento da compra efetuada, sendo posteriormente atribuído um código de acesso específico ao item reservado. Na altura pretendida para o usufruto da reserva efetuada, será requerido ao utilizador um código de acesso, juntamente com alguns dados pessoais disponibilizados na primeira etapa, que, caso corretos, irão conceder ao utilizador acesso ao quarto reservado em seu nome;
- **Autorização por parte do sistema**: Nesta etapa, os dados inseridos na fase de identificação e autenticação são comparados com os dados guardados na altura do registo e reserva do espaço. Caso haja um "*match*" total desses dados, será concedido o acesso ao quarto, podendo, assim, o utilizador usufruir da sua compra na totalidade;

- **Auditoria/Monitorização da atividade do utilizador**: Em paralelo a estas etapas, existe a auditoria/monitorização das reservas e dos espaços arrendados. Este processo é realizado pelo proprietário/administrador do(s) quarto(s), tendo este o poder de adicionar ou remover quartos, ou até mesmo alterar toda a informação disponibilizada acerca destes.

Neste processo, é possível identificar a presença de 4 elementos principais: o servidor, o proprietário/administrador, o utilizador e o quarto. Como referido anteriormente, a arquitetura proposta segue o modelo Cliente/Servidor (Secção 2.5). Este modelo, no caso em estudo, é composto por um servidor central (servidor base de dados + servidor da plataforma de reservas), que tem a função de responder aos pedidos feitos pelos seus clientes.

4.1.2 Arquitetura do Sistema Implementado

Na Figura 4.1 foi apresentada uma solução em que existe apenas um servidor (Servidor WEB + Servidor Base de Dados) para gerir a comunicação na rede de equipamentos do sistema proposto. Isto deve-se ao facto de inicialmente, ser necessário escolher uma tipologia de arquitetura (Secção 2.6) que facilite e generalize todo o tipo de interação entre diversos dispositivos.

Apesar das desvantagens claras de uma arquitetura centralizada, esta demonstra ser a solução mais adequada para o caso em estudo. Embora todo o sistema esteja apenas dependente de um único servidor, consegue-se garantir uma maior segurança nos dados transmitidos. Consegue-se também garantir, com este tipo de arquitetura, uma maior segurança de comunicação entre os clientes e o servidor, ao serem evitadas ligações com outros equipamentos vulneráveis a ataques informáticos externos na mesma rede.

4.1.3 Comunicação entre equipamentos

Como foi referido no Capítulo 3, na Figura 3.1 o sistema proposto tem previsto a interação entre 3 clientes principais (utilizador, proprietário/administrador e quarto) e um servidor central. Esta secção tem por vista estabelecer um meio de comunicação entre o cliente principal desta solução, o cliente "Quarto", e outros equipamentos necessários, de forma a se conseguir a comunicação entre o Quarto e o servidor do sistema.

O cliente "Quarto", referido anteriormente, na verdade consiste na fechadura do espaço que permite o acesso ao quarto reservado pelo utilizador. Como a fechadura, por si só, não tem capacidade de se ligar diretamente à Internet, é facultativo, existir, a nível intermédio, um *access point* (*router*) ou uma operadora telefónica que consiga estabelecer essa ligação (Ver Figura 4.2).

Tendo em consideração as vantagens de uma comunicação "sem fios" entre equipamentos, os protocolos/tecnologias existentes que satisfazem as necessidades impostas são:

- **Wi-Fi** (IEEE 802.11);
- **GSM** (*Global System for Mobile communications*)/**GPRS** (*General Packet Radio Service*).

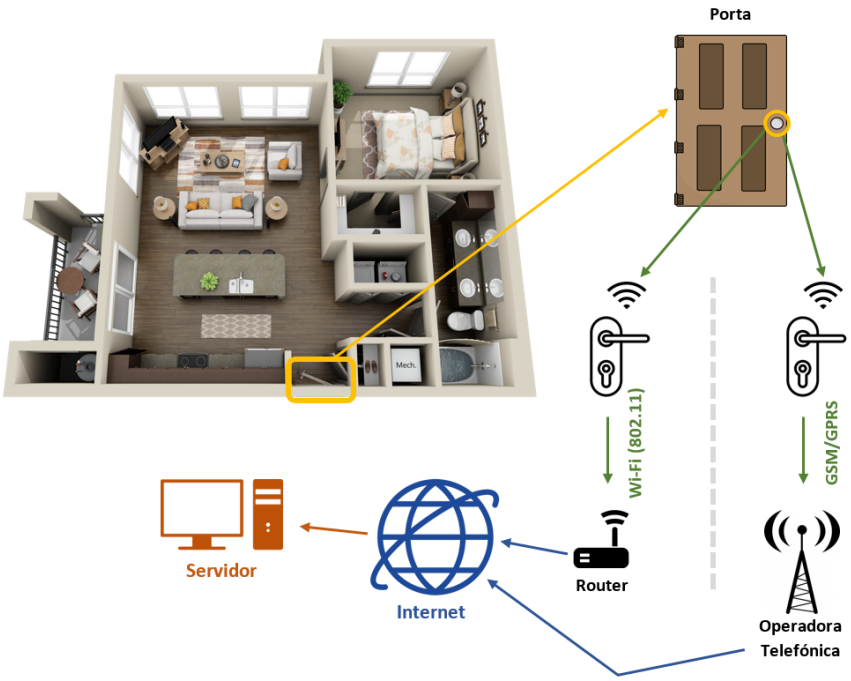


Figura 4.2: Comunicação Fechadura - Servidor [58]. (Adaptada)

Tendo em conta os aspetos demonstrados nas Tabelas 2.1 e 2.2, sobre algumas características acerca dos protocolos GSM/GPRS e Wi-Fi (802.11), é possível concluir que existe possibilidade de aplicar tanto uma como a outra, sendo que cada uma destas impõe algumas condições específicas para o seu funcionamento.

O protocolo GPRS necessita de ter associado um cartão SIM com um tarifário móvel que permita ligação à rede Internet, sendo, ao fim de cada mês, aplicada uma tarifa pelo uso do serviço. Esta opção também tem a desvantagem de ter uma velocidade de transmissão de dados muito lenta, comparativamente com a fornecida pelo protocolo Wi-Fi (802.11).

O protocolo Wi-Fi (802.11), por sua vez, apenas necessita, para estabelecer comunicação com outros equipamentos, de um *access point* ligado à rede Internet. Cada *access point* permite a ligação de vários clientes de uma só vez, tornando-se bastante mais vantajoso neste aspeto, por permitir a redução do número de equipamentos necessários. O único custo inicial a ter em conta reside na compra dos *access points* (*routers*) necessários, tendo a tarifa para acesso à rede Internet um custo mensal, que pode não depender do número de *routers* disponibilizados. Este serviço, como referido no parágrafo anterior, também permite uma maior velocidade de transferência de dados, garantindo uma velocidade de comunicação entre equipamentos bastante mais elevada.

A comunicação entre os equipamentos-cliente e o servidor central do sistema é feita com o auxílio de outro protocolo, o protocolo TCP/IP (*Transmission Control Protocol/Internet Protocol* - Secção 2.8).

4.2 *Software*

Esta secção está focada no *software* desenvolvido para a solução proposta, sendo este constituído por:

- Base de Dados do sistema;
- Plataforma de Reservas desenvolvida para a reserva dos espaços disponíveis, respetivo pagamento e para a monitorização das reservas em vigor e da informação disponibilizada sobre cada alojamento;
- Programa desenvolvido para os microcontroladores estudados (NodeMcu/ESP8266 e SIM900);
- Configuração do XAMPP como servidor de *emails*, servidor WEB e como gestor MySQL;

Nas secções seguintes, irão ser abordados todos estes pontos essenciais para um bom funcionamento do sistema, sendo impreterível salientar a importância da base de dados do sistema, que irá conter toda a informação relativa às reservas, aos quartos e aos dados necessários para o funcionamento esperado da fechadura de cada alojamento.

4.2.1 Base de Dados do Sistema

Para esta dissertação, tendo em consideração as necessidades de automatização do processo de reservas e controlo de acessos, torna-se indispensável a utilização de uma base de dados relacional para armazenamento da informação em fluxo no sistema. Sabendo que o intuito da base de dados é servir um sistema de reservas para indústria hoteleira, propõe-se, de seguida (Figura 4.3), uma lista de atributos da Relação Universal que se pretende adquirir para o bom funcionamento da solução:

Figura 4.3: Atributos em conta para construção da Base de Dados.

O passo seguinte para a construção da base de dados prende-se na atribuição de dependências funcionais entre os vários atributos da Figura 4.3. A dependência funcional é representada com uma seta que indica, no sentido para o qual aponta, "existe apenas um e só um". Sendo assim, assume-se que cada cliente, como seria de esperar, tem apenas um e um só nome e apelido e um e um só NIF (Número de Identificação Fiscal).

Na plataforma de reservas, para além dos dados referidos na linha anterior, o cliente tem oportunidade de colocar no seu registo um *email*, uma *password*, um número de telefone, um país, uma cidade, um código postal e uma morada. Para cada parâmetro apenas é permitido colocar uma e uma só opção.

O código *hash*, presente na lista de atributos, refere-se à *password* encriptada segundo um algoritmo do mesmo nome. Se existe uma e só uma *password*, também existe apenas uma e uma só *hash* para cada número de cliente. O estatuto apenas se refere ao tipo de utilizador/cliente da plataforma de reservas. Apenas foram considerados, para o caso

em questão, dois tipos de utilizadores: um do tipo cliente e outro do tipo administrador. Esses estatutos apenas vão modificar o tipo de informação apresentada no *login* do utilizador no sistema. Ao administrador serão apresentados os dados relativos a todas a reservas em vigor e toda a informação disponibilizada na plataforma sobre os alojamentos disponíveis. Ao cliente, apenas será apresentada informação sobre o seu histórico de reservas neste serviço.

Após a escolha do quarto desejado e o registo no sistema, é atribuído a cada cliente um número de reserva, ou seja, para cada número de reserva existe um e apenas um número de cliente. Ao número de reserva estão também associados as datas de *check-in* e *check-out*, o montante da estadia, resultante do número de dias a multiplicar pelo preço individual de cada quarto por dia, o número do quarto escolhido na reserva, um código de acesso gerado automaticamente pelo sistema e um *payment ID*, derivado do pagamento da reserva via "PayPal" (para cada número de reserva existe um e só um elemento de cada parâmetro apresentado). O estado de ocupação (ocupado ou livre) também está associado ao número de reserva. Este parâmetro permite diferenciar as reservas pendentes das reservas "terminadas".

Um estabelecimento hoteleiro, como é natural, possui mais que um quarto, ou mais que um alojamento para posterior reserva. Para isso, é necessário identificar na plataforma de reservas as características principais de cada quarto, aliadas com uma imagem alusiva do mesmo. Cada número de quarto apenas pode ter um e um só tipo (*single*, *double*, *suite*, entre outros), um e um só preço, uma e uma só capacidade (número de pessoas que podem dormir no quarto, num sítio adequado para o efeito) e uma e uma só imagem (pode ter mais imagens, mas neste caso considera-se que existe apenas uma imagem para cada quarto).

Para cada data de entrada, hora de entrada e número de quarto existe apenas uma e só uma reserva associada. Esta informação existe para monitorização da atividade do cliente no alojamento.

Para obter um sistema de reservas funcional a nível empresarial, teve de ser considerada a parte relativa aos pagamentos e a sua respetiva confirmação. Para isso, foram considerados 4 atributos essenciais ao pagamento de uma compra via "PayPal": O *currency code*, o *transaction ID*, o montante da estadia e o *payment status*. Sabendo que o *currency code* indica o tipo de moeda em que vai ser feita a transação, é possível afirmar que existe apenas um e um só *currency code* para cada *payment ID*.

Após o pagamento da reserva no "PayPal", existe um código que é enviado para o servidor do sistema de reservas e que é posteriormente reenviado para o "PayPal", anexado com o *identity token* da empresa (*string* que identifica a conta do empresário no "PayPal"). Esse código é denominado de *transaction ID* e pode concluir-se que existe também apenas um e só um associado a cada *payment ID*. O montante da estadia também é apenas um e só um para cada *payment ID*, por apenas se fazer um pagamento por reserva. Finalmente, após cada cliente ter efetuado a sua reserva, a plataforma de reservas redireciona diretamente o cliente para uma página de pagamento no "PayPal".

Na eventualidade da compra ter sido bem sucedida, é necessário o sistema se aperceber da confirmação do pagamento para enviar um *email* ao cliente com os dados da sua reserva, juntamente com o código de acesso válido para as datas de *check-in* e *check-out* predeterminadas.

Com isto, estão determinadas as dependências funcionais entre todos os atributos necessários para o bom funcionamento da solução. Na Figura 4.4 está representado o diagrama de dependências funcionais do sistema de reservas desta dissertação [17].

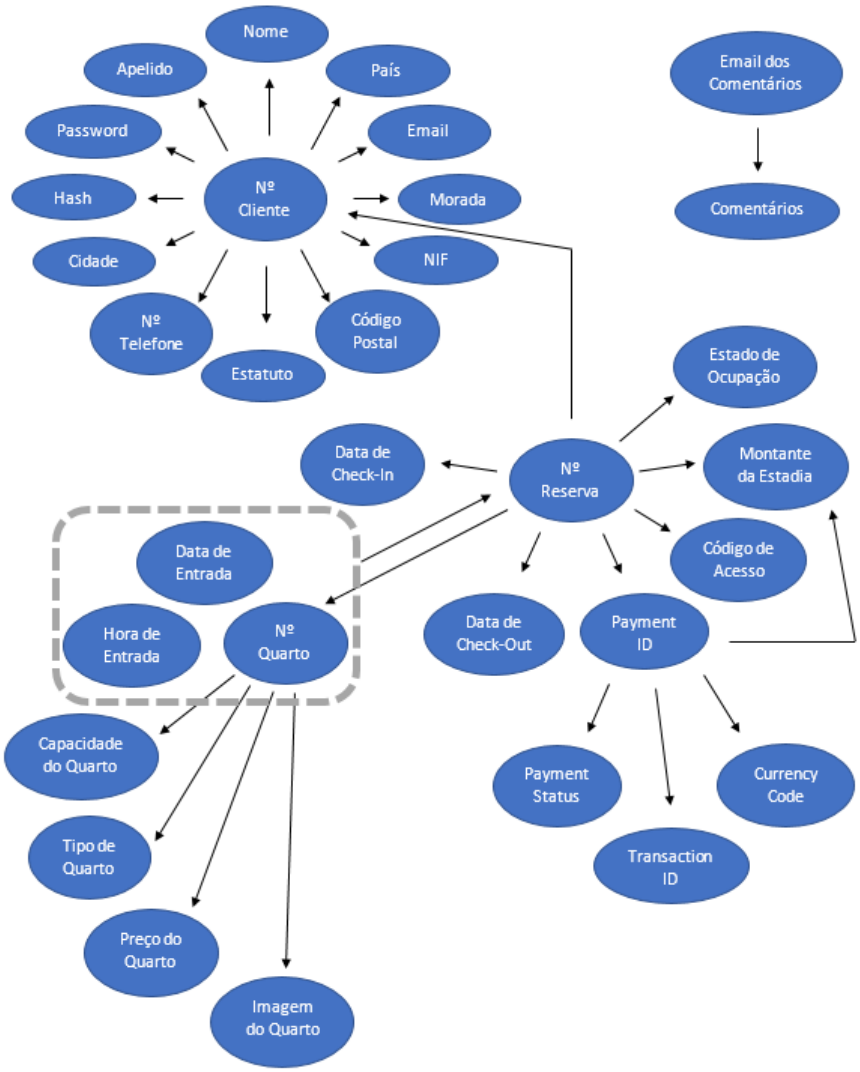


Figura 4.4: Diagrama de dependências funcionais da Relação Universal.

R(Atributos presentes na 4.3)

Determinantes
1.<Nº Cliente>, 2.<Nº Reserva>, 3.<*Payment ID*>, 4.<Nº Quarto>, 5.<*Email* dos Comentários>, 6.<Data de Entrada, Hora de Entrada, Nº Quarto>
Chaves Candidatas
1.<Data Entrada, Hora Entrada, Nº Quarto>

A relação universal "R", com todos os atributos considerados para o sistema de reservas, não se encontra na Forma Normal de *Boyce Codd* (FNBC). Isso acontece, pois nem todos os determinantes da relação são chaves candidatas dessa mesma relação.

Para obter uma relação normalizada, é necessário seguir um processo iterativo de decomposição de tabelas/relações em tabelas/relações mais pequenas. Numa primeira iteração procurou-se dividir a tabela/relação universal "R" em três relações: R1 (Figura 4.5), R2 (Figura 4.6) e R3 (Figura 4.11).

Relação R1

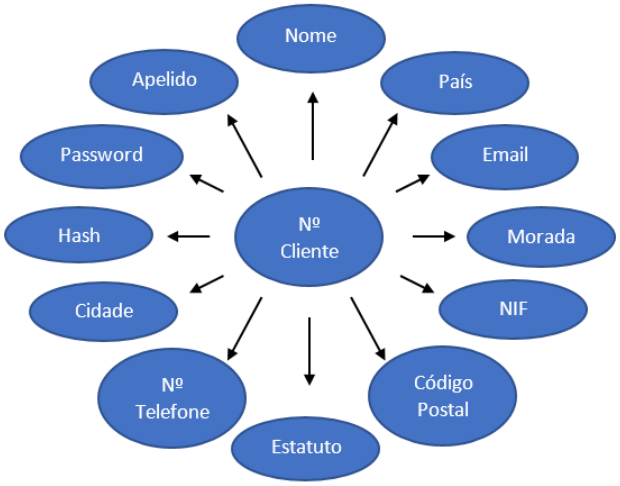


Figura 4.5: Diagrama de dependências funcionais da Relação R1.

R1(Nº Cliente, Nome, Apelido, *Password*, *Hash*, Cidade, Nº Telefone, Estatuto, Código Postal, NIF, Morada, *Email*, País)

Determinantes
1.<Nº Cliente>
Chaves Candidatas
1.<Nº Cliente>

Como é possível visualizar acima, o determinante e a chave candidata da relação R1 são iguais, pelo que se pode concluir que a relação R1 está normalizada. Esta relação dá origem a uma tabela da base de dados que se chama Utilizadores. Esta tabela vai reter toda a informação sobre os clientes registados no sistema de reservas, segundo os atributos ilustrados na Figura 4.5. A tabela, por sua vez, tem previsto o seguinte formato (Tabela 4.1):

Tabela 4.1: Tabela "Utilizadores" da Base de Dados

Nº Cliente #	Nome	Apelido	*Email*	*Password*	*Hash*	Nº Telefone	NIF	País	Cidade	Morada	Código Postal	Estatuto

Relação R2

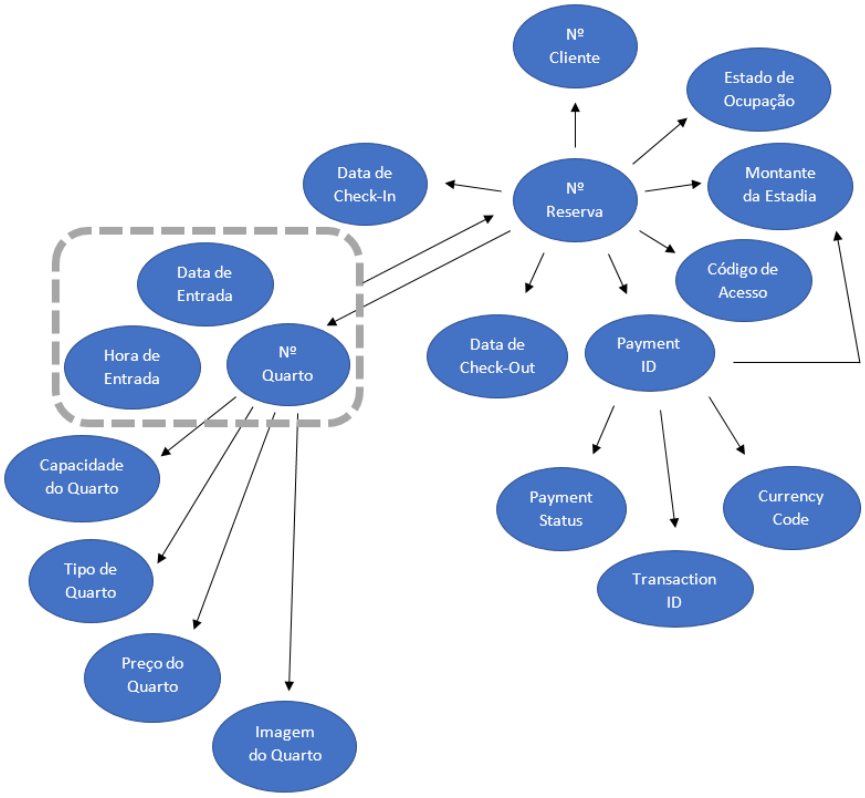


Figura 4.6: Diagrama de dependências funcionais da Relação R2.

R2(Nº Reserva, Nº Cliente, Data de *Check-In*, Data de *Check-Out*, Código de Acesso, Montante da Estadia, Nº Quarto, Capacidade do Quarto, Tipo de Quarto, Preço do Quarto, Imagem do Quarto, Estado de Ocupação, *Payment ID*, *Payment Status*, *Transaction ID*, *Currency Code*, Data de Entrada, Hora de Entrada)

Determinantes
1.<Nº Reserva>, 2.<Nº Quarto>, 3.<*Payment ID*>,
4.<Data de Entrada, Hora de Entrada, Nº Quarto>
Chaves Candidatas
1.<Data de Entrada, Hora de Entrada, Nº Quarto>

Visto que nem todos os determinantes são chaves candidatas da relação R2, é possível concluir que esta relação não se encontra normalizada segundo a FNBC. Por essa razão, é necessário subdividir a relação R2 em quatro outras: a relação R2.1 (Figura 4.7), a relação R2.2 (Figura 4.8), a relação R2.3 (Figura 4.9) e a relação R2.4 (Figura 4.10).

Relação R2.1

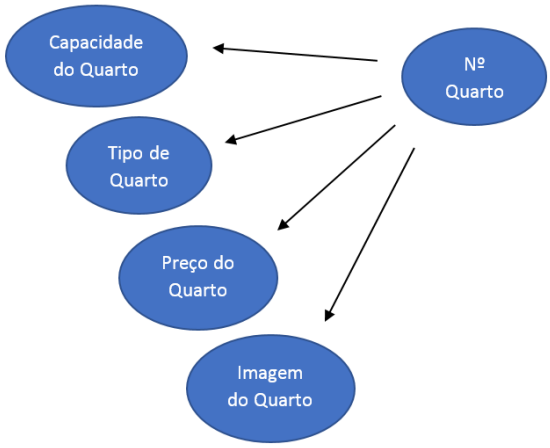


Figura 4.7: Diagrama de dependências funcionais da Relação R2.1.

R2.1(Nº Quarto, Capacidade do Quarto, Tipo de Quarto, Preço do Quarto, Imagem do Quarto)

Determinantes
1.<Nº Quarto>
Chaves Candidatas
1.<Nº Quarto>

Visto os determinantes da relação 2.1 serem iguais às suas chaves candidatas, é possível concluir que esta relação está normalizada. Isto significa que existe uma tabela da base de dados que vai conter os dados relativos a esta relação. Sabendo que esta tabela (Tabela "Quartos") tem toda a informação sobre os quartos disponíveis para aluguer, o formato proposto para a mesma é semelhante ao da tabela seguinte (Tabela 4.2):

Tabela 4.2: Tabela "Quartos" da Base de Dados

Nº Quarto #	Tipo de Quarto	Imagem do Quarto	Capacidade do Quarto	Preço do Quarto

Relação R2.2

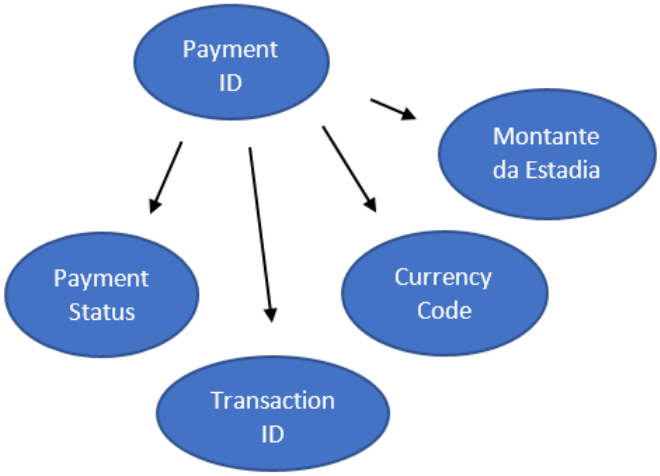


Figura 4.8: Diagrama de dependências funcionais da Relação R2.2.

R2.2(*Payment ID*, *Payment Status*, *Transaction ID*, *Currency Code*, Montante da Estadia)

Determinantes
1.<*Payment ID*>
Chaves Candidatas
1.<*Payment ID*>

Esta relação, tal como a anterior, está normalizada, por ter os determinantes iguais às chaves candidatas. Por essa razão, esta relação obriga à criação de uma nova tabela da base de dados chamada "Pagamentos". Esta tabela irá, principalmente, receber informação vinda da comunicação entre o sistema de reservas e a interface de pagamentos "PayPal", daí o nome dos atributos serem bastante específicos e estarem em inglês. A tabela seguinte (Tabela 4.3) mostra um exemplo de estrutura desta tabela:

Tabela 4.3: Tabela "Pagamentos" da Base de Dados

Payment ID #	Transaction ID	Currency Code	Montante da Estadia	Payment Status

Relação R2.3

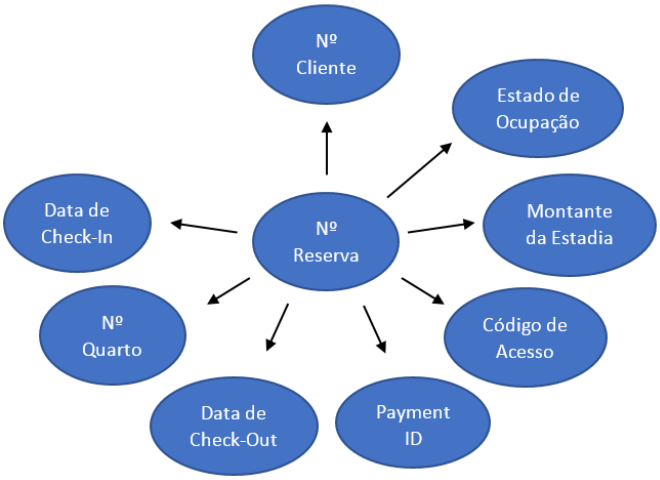


Figura 4.9: Diagrama de dependências funcionais da Relação R2.3.

R2.3(Nº Reserva, Nº Cliente, Data de *Check-In*, Nº Quarto, Data de *Check-Out*, *Payment ID*, Código de Acesso, Montante da Estadia, Estado de Ocupação)

Determinantes
1.<Nº Reserva>
Chaves Candidatas
1.<Nº Reserva>

A última sub-divisão da relação "R2" consiste numa relação com todos os atributos relacionados à reserva de um quarto. Esta relação, tal como as anteriores, está normalizada e dá origem a uma nova tabela da base de dados, a tabela "Reservas". A Tabela 4.4 consiste num exemplo proposto para esta nova tabela "Reservas":

Tabela 4.4: Tabela "Reservas" da Base de Dados

Nº Reserva #	Data de *Check-In*	Data de *Check-Out*	Nº Quarto	Nº Cliente	Código de Acesso	Montante da Estadia	*Payment ID*	Estado de Ocupação

Relação R2.4

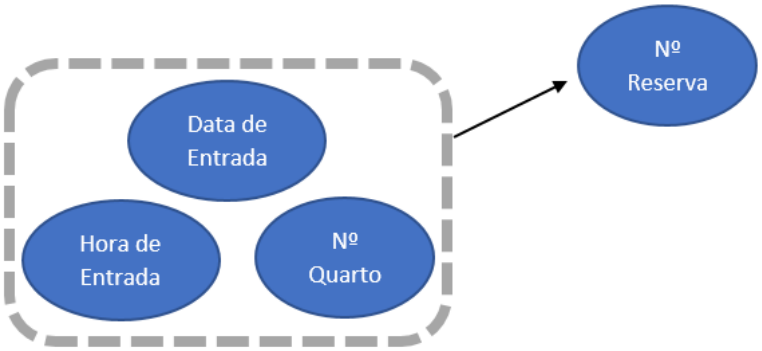


Figura 4.10: Diagrama de dependências funcionais da Relação R2.4.

R2.4(Data de Entrada, Hora de Entrada, Nº Quarto, Nº Reserva)

Determinantes
1.<Data de Entrada, Hora de Entrada, Nº Quarto>
Chaves Candidatas
1.<Data de Entrada, Hora de Entrada, Nº Quarto>

Esta relação está normalizada por ter os seus determinantes iguais às chaves candidatas. Desta forma, a relação acima exposta leva à criação de uma nova tabela da base de dados, denominada, Tabela "Histórico". Esta tabela tem como objetivo a monitorização da atividade do cliente no alojamento (com sensor que deteta abertura da porta). A Tabela 4.5) mostra um exemplo de estrutura desta tabela:

Tabela 4.5: Tabela "Histórico" da Base de Dados

Data de Entrada #	**Hora de Entrada #**	**Nº Quarto #**	**Nº Reserva**

Relação R3

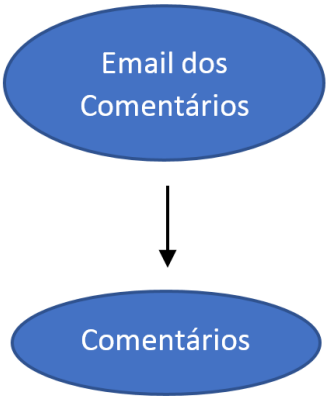


Figura 4.11: Diagrama de dependências funcionais da Relação R3.

R3(*Email* dos Comentários, Comentários)

Determinantes
1.<*Email* dos Comentários>
Chaves Candidatas
1.<*Email* dos Comentários>

Por último, a terceira sub-divisão da relação universal "R" refere-se aos *emails* mandados pelos clientes da plataforma de reservas, que não precisam de obrigatoriamente estarem registados na tabela "Utilizadores". Esta relação (R3) apenas visa registar as dúvidas sentidas pelos utilizadores da plataforma de reservas, sendo estas posteriormente respondidas pelo administrador do sistema. A relação R3, por ter os seus determinantes idênticos às suas chaves candidatas, encontra-se normalizada e dá origem à última tabela da base de dados denominada "Comentários". Esta tabela é bastante simples e segue a estrutura da tabela seguinte (Tabela 4.6):

Tabela 4.6: Tabela "Comentários" da Base de Dados

***Email* dos Comentários #**	**Comentários**

4.2.2 Plataforma Desenvolvida

Para o bom funcionamento de uma solução que tem por finalidade oferecer ao cliente um sistema funcional de reservas automatizado, a necessidade de desenvolvimento de uma plataforma de reservas é imprescindível. Esta plataforma é utilizada como interface intermediária entre os intervenientes do sistema (Cliente "Turista" e Administrador "Proprietário") e a base de dados do mesmo.

O Cliente desta solução recorre aos serviços oferecidos pela plataforma de reservas no momento da reserva do alojamento pretendido (para registo dos dados relativos à reserva

e para registo da sua informação pessoal) e para consulta das suas reservas já feitas neste sistema.

O Administrador, como entidade superior, tem a capacidade de poder monitorizar todas as reservas em vigor no sistema, bem como gerir as faturas entregues a cada cliente. Para além destas funções, este pode alterar toda a informação disponibilizada sobre os quartos/alojamentos disponíveis na plataforma.

Para diferenciar os utilizadores clientes do(s) utilizador(es) administrador(es) foi necessário desenvolver uma página de *login* que permite, através das credenciais de *login* (*email* e *password*), diferenciar os diferentes tipos de utilizadores existentes na plataforma.

A Figura 4.12 existe com o intuito de ilustrar o funcionamento da plataforma de reservas desta solução, com todas as ações possíveis de visualizar no decorrer da sua utilização [59].

De forma a estruturar o raciocínio tomado no desenvolvimento da plataforma de reservas, as secções seguintes encontram-se divididas segundo as diversas páginas da plataforma WEB:

1. Página Inicial;
2. Página de requisitos da Reserva;
3. Página de *Login* do Utilizador;
4. Página de Apresentação dos Quartos Disponíveis;
5. Página - Carrinho de Compras;
6. Página de Confirmação dos Dados e Pagamento;
7. Página de Sucesso/Página de Erro.

Para além destes fatores tidos em conta no desenvolvimento da plataforma de reservas, também foi necessário pensar em aspetos técnicos fundamentais para a implementação da solução em ambiente real.

Sabendo de antemão que a plataforma de reservas precisa de estar operacional 24 horas por dia, a necessidade de utilizar um servidor dedicado para processar os pedidos de acesso às páginas WEB, bem como à base de dados do sistema, é indispensável.

Para teste do funcionamento da solução foi utilizado um computador servidor disponível no DEM (Departamento de Engenharia Mecânica). O acesso à plataforma a partir de qualquer computador é garantido, nesta situação, com a atribuição de um endereço IP público ao servidor do sistema.

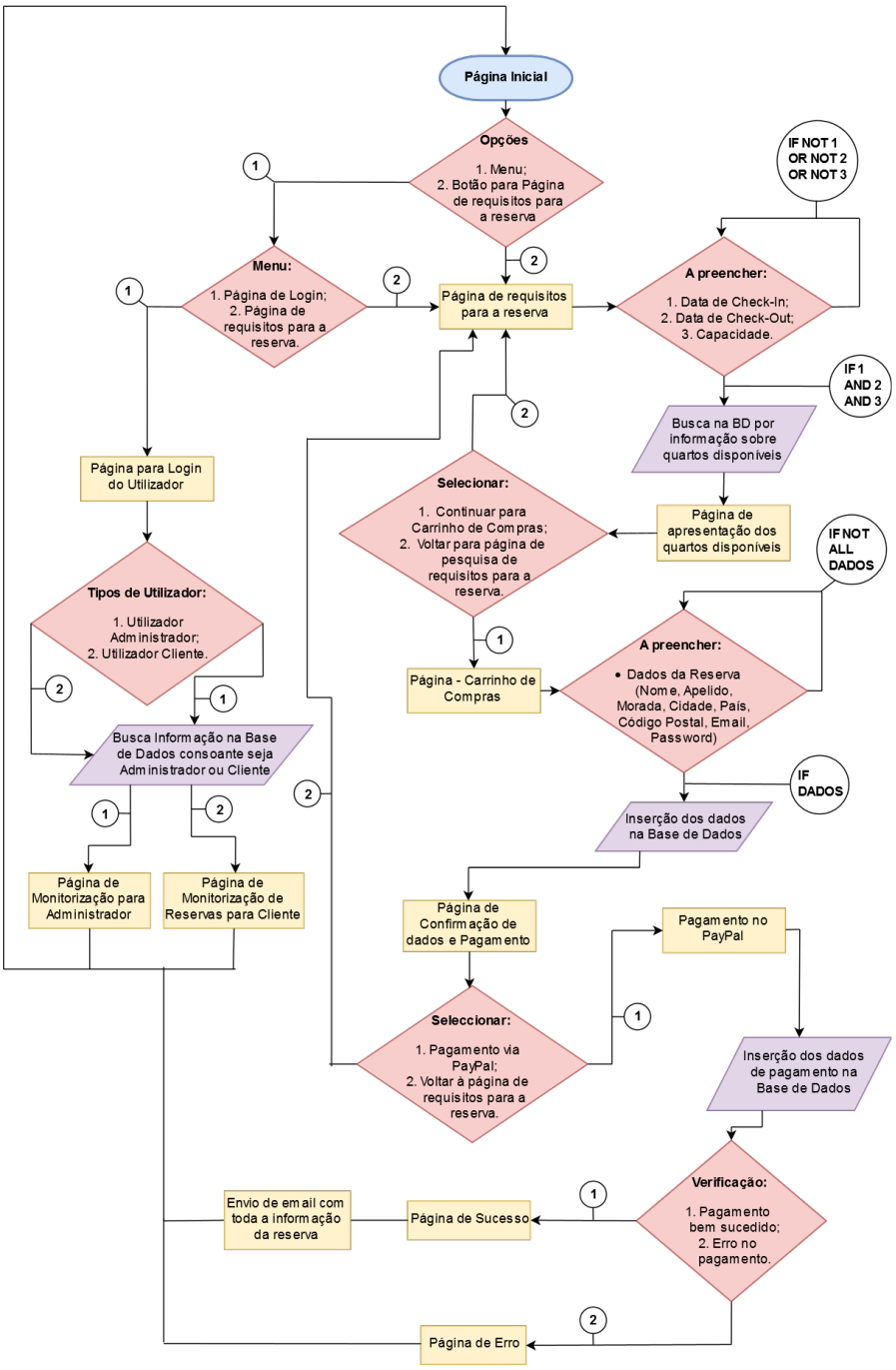


Figura 4.12: Fluxograma de funcionamento da Plataforma de Reservas.

Qualquer equipamento ligado em rede possui um endereço IP associado. Relativamente a endereços IP, existem dois tipos de endereços: os públicos e os privados.

Sendo a maioria dos endereços IP endereços públicos, o acesso a qualquer equipamento através da Internet torna-se bastante facilitado. Um exemplo de aplicação de endereços públicos está presente no quotidiano da maioria das pessoas. Como se sabe, é comum existir nas redes domésticas um *router*/*access point* que faz fronteira entre os equipamentos de casa e a Internet. Esse *router*, por norma, tem um IP público que permite a comunicação entre os equipamentos de casa e o mundo (ou seja, torna os equipamentos de casa acessíveis publicamente através da Internet).

Os endereços privados, por sua vez, não permitem acesso direto à Internet. Esse acesso apenas é possível recorrendo a mecanismos de NAT (*Network Address Translation*), que traduzem um endereço IP privado num endereço público. Um exemplo de aplicação deste tipo de endereços, recorrendo ao exemplo anterior, consiste nos endereços dos equipamentos de casa de uma rede doméstica. Esses equipamentos apenas conseguem acesso à Internet através do *router*/*access point* de casa.

Os endereços IP públicos são, por norma, geridos por uma operadora de rede e permitem identificar univocamente uma máquina na Internet. A Figura 4.13 ilustra, de forma simplificada, a aplicabilidade dos endereços IP referidos anteriormente [60].

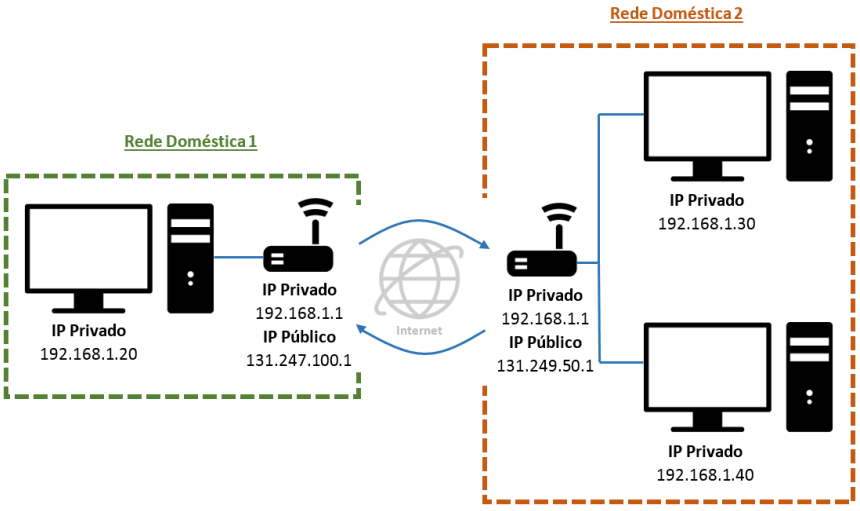


Figura 4.13: Endereços IP Públicos e Privados.

Para além da necessidade de atribuir um endereço IP público ao servidor do sistema, a necessidade de ter um servidor capaz de conceder acesso a páginas WEB e que permite a comunicação entre a plataforma de reservas e a base de dados do sistema é fundamental para um bom funcionamento da solução.

Uma forma de permitir o acesso à informação armazenada no servidor consiste na instalação de um *software* denominado XAMPP.

Este *software* é constituído por um conjunto de funcionalidades úteis para esta dissertação, como: um servidor WEB denominado "Apache", um gestor de bases de dados MySQL e um servidor de *emails* chamado "Mercury".

Para complemento da informação cedida, o Apêndice A contém uma série de *prints* das diversas páginas da plataforma.

Página Inicial

A Página Inicial da plataforma de reservas existe com o intuito de apresentar a empresa a novos potenciais clientes. Nesta página encontra-se um pequeno texto descritivo da empresa, cujo foco assenta no desenvolvimento de soluções que procuram a automatização do processo de reservas e do controlo de acessos na indústria hoteleira.

Para além do texto introdutório, esta página também serve como porta de acesso para outras duas: uma de requisitos para a reserva e outra de *login* para os utilizadores do sistema. O acesso às duas páginas pode ser feito de duas formas: através de um menu no canto superior direito da página, ou através de um botão no fim do texto de introdução à empresa. O menu, como se pode visualizar na Figura 4.12 concede acesso às paginas de *login* e à de requisitos da reserva, sendo que o botão apenas permite o acesso à página de requisitos da reserva (Funcionamento resumido na Figura 4.14).

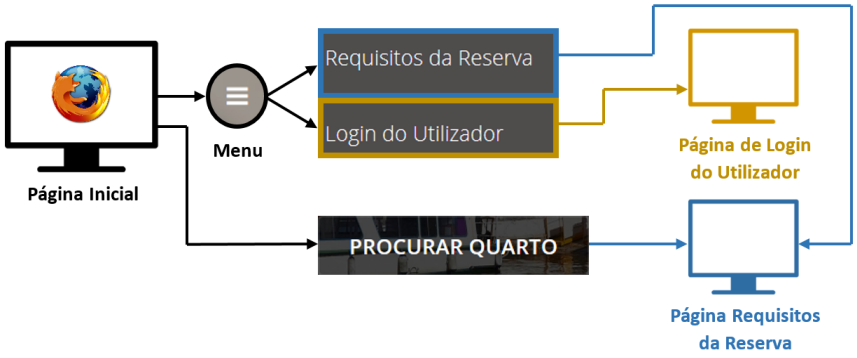


Figura 4.14: Diagrama de funcionamento da Página Inicial.

Página de Requisitos da Reserva

Esta página de requisitos foi desenvolvida com o intuito de facilitar a busca do cliente pelo quarto/alojamento ideal para a sua estadia. Para a pesquisa de determinado quarto/alojamento, é necessário ter em conta a sua disponibilidade e o número de pessoas que cada quarto pode albergar, sabendo que essas pessoas têm de dormir num local apropriado para o efeito. De forma a colmatar estas premissas, foi colocado na página de requisitos um pequeno formulário de preenchimento obrigatório com os campos:

- Data de *Check-In*;
- Data de *Check-Out*;
- Capacidade suportada.

Na eventualidade do cliente tentar submeter a informação do formulário com campos em branco, a própria página de requisitos avisa o cliente para preencher os dados em falta, de forma a poder continuar com o processo de reserva.

No momento de submissão dos dados introduzidos inicia-se o processo de comunicação com a base de dados da solução. Todos os pedidos feitos nesta comunicação partem da página de requisitos com destino à base de dados. Estes pedidos seguem na forma

de *queries* SQL, com vista na obtenção de informação vital ao bom funcionamento do sistema.

Logo após a submissão dos dados, segue uma *query* para a Tabela "Reservas" com o objetivo de adquirir os quartos disponíveis entre as datas de *check-in* e *check-out* pretendidas pelo cliente. Depois de processar o pedido, a base de dados responde para a página com a informação desejada, ou seja, com o nome dos quartos disponíveis entre as datas requisitadas.

Na tentativa de reduzir o número de quartos obtidos na pesquisa anterior, é enviada uma segunda *query* para a base de dados da solução. Este segundo pedido dirige-se à tabela "Quartos" e tem o objetivo de saber quais dos quartos/alojamentos resultantes da última pesquisa satisfazem as necessidades do cliente em relação à capacidade suportada. Após o processamento da informação pedida, a base de dados responde com os quartos disponíveis e com a capacidade pretendida pelo cliente (Ver Figura 4.15).

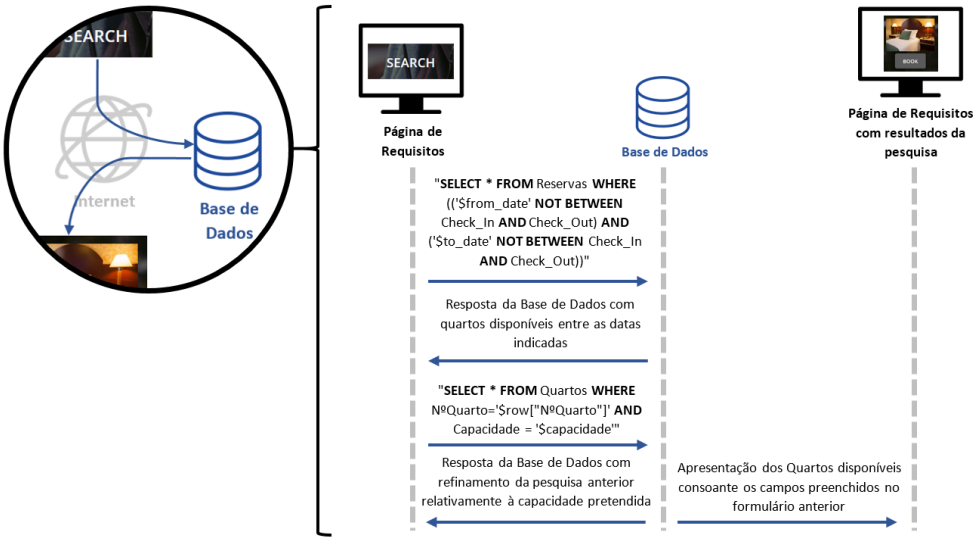


Figura 4.15: Diagrama de interações da comunicação com a BD na Página de Requisitos.

Posto isto, sabendo quais os quartos que atendem às necessidades impostas no formulário da página, é essencial disponibilizar alguma informação adicional sobre os mesmos. Essa informação tem o objetivo de ajudar o cliente a escolher de forma consciente qual o quarto que se adequa às suas necessidades, tanto a nível de estadia, como a nível económico.

De maneira a dar seguimento ao processo de reservas, cada linha da tabela tem um botão associado, com uma hiperligação para a página seguinte, a página de "Carrinho de Compras" (Funcionamento resumido na Figura 4.16).

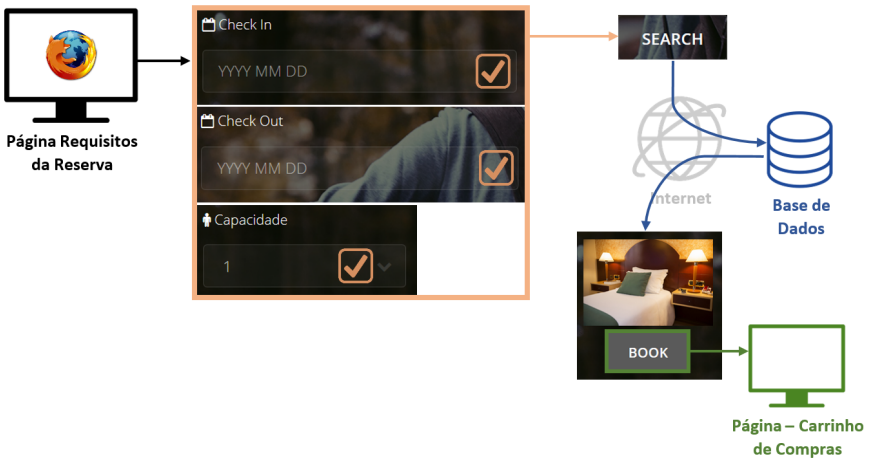


Figura 4.16: Diagrama de funcionamento da Página de Requisitos.

Página - Carrinho de Compras

A página de "Carrinho de Compras", como referido anteriormente, existe com o intuito de dar a conhecer ao cliente algo mais sobre o quarto/alojamento escolhido. Para além dessa funcionalidade, esta página dispõe de um formulário de preenchimento obrigatório, que permite ao cliente fazer o seu registo na base de dados do sistema, bem como avançar para o pagamento da sua reserva.

No preenchimento do formulário é necessário ter especial atenção ao preenchimento dos dados, de maneira a não deixar campos em branco, ou até mesmo no digitar de dados num formato indesejado. A página está encarregue de alertar o cliente na eventualidade de um destes casos acontecer. O processo de pagamento da reserva apenas pode ser retomado após a correção das falhas identificadas.

O avanço para a página de pagamento da reserva pode ser feito através do preenchimento de dois formulários: um para clientes já registados no sistema e outro para novos clientes. O formulário para um novo cliente do sistema contém uma lista com os seguintes atributos:

- Nome;
- Apelido;
- *Email*;
- *Password*;
- Número de Telefone;
- NIF;
- Morada;
- Cidade;
- Código Postal;

- País.

Após a submissão dos dados é iniciada a comunicação com a base de dados da solução. Esta comunicação visa o registo da informação relativa ao cliente na Tabela "Utilizadores", definida na secção 4.2.1. Para tal, é necessário enviar uma *query* de inserção para a base de dados, com todos os campos associados às respetivas colunas da tabela "Utilizadores". Para evitar futuros problemas no *login* do utilizador e na reserva de determinado espaço, um cliente registado no sistema com um determinado *email* não consegue fazer um novo registo utilizando esse mesmo *email*.

O segundo formulário foi desenvolvido para clientes já registados no sistema. Este formulário apenas é composto pelo *Email* e *Password* do cliente, previamente escolhidos no primeiro registo do cliente na plataforma de reservas. A submissão destes campos, tal como no formulário anterior, permite o avanço para a página de confirmação de dados e pagamento da reserva. (Funcionamento resumido na Figura 4.17)

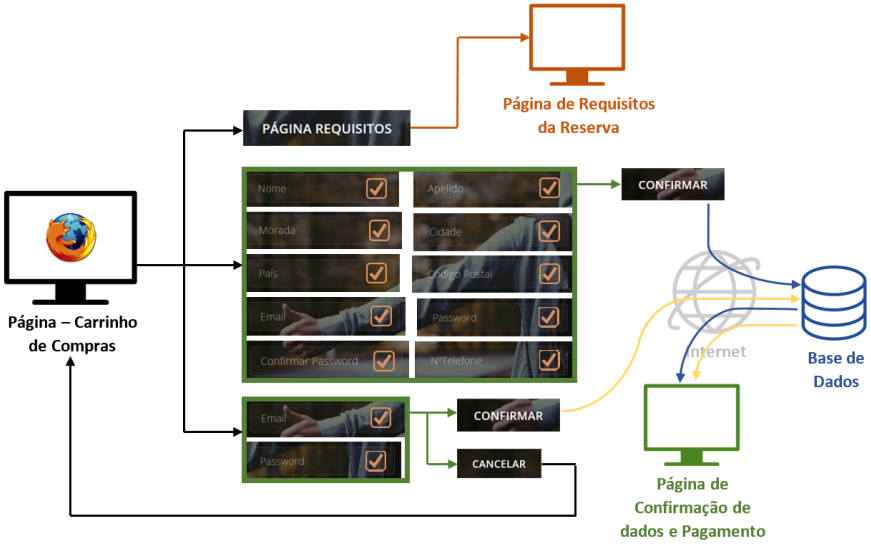


Figura 4.17: Diagrama de funcionamento da Página - Carrinho de Compras.

Na Figura 4.18, encontra-se ilustrada a comunicação entre a página de "Carrinho de Compras" e a base de dados desta solução.

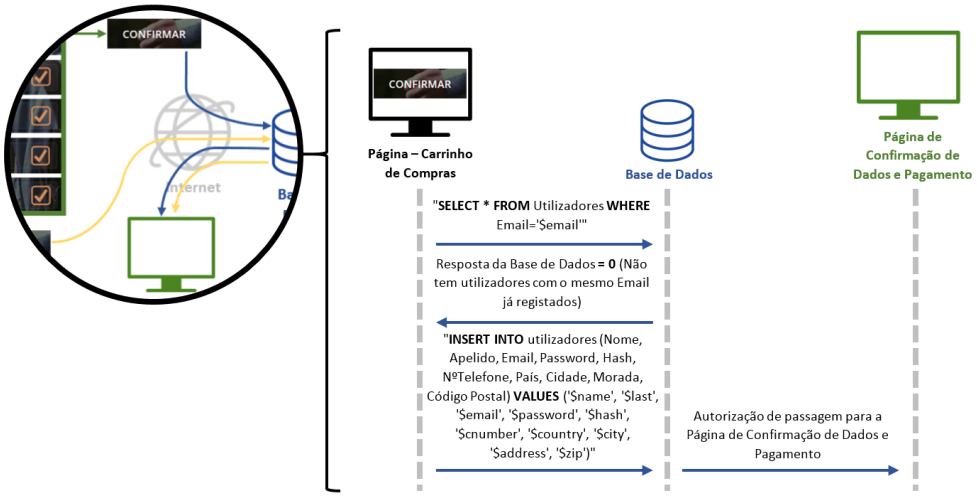


Figura 4.18: Diagrama de interações da comunicação com a BD na Página - Carrinho de Compras.

Página de Confirmação de Dados e Pagamento

A etapa posterior ao registo do cliente na base de dados do sistema, ou até mesmo à submissão do formulário de *login* (para um cliente já registado no sistema) consiste na confirmação dos dados da reserva e seu respetivo pagamento.

Esta página, tal como o nome indica, está dividida em duas partes: uma lista de informação relativa ao processo de reserva de determinado cliente e um botão de pagamento via "PayPal". O preenchimento da lista tem em conta a informação armazenada nas etapas anteriores. Esta lista é constituída pelos seguintes itens:

- Data de *Check-In*;
- Data de *Check-Out*;
- Capacidade Suportada;
- Número do Quarto;
- Tipo de Quarto;
- Nome;
- Apelido;
- País;
- Cidade;
- Morada;
- Código Postal;

- *Email*;
- Número de Telefone;
- Montante da Estadia.

O botão do pagamento, por sua vez, permite redirecionar o cliente para uma página do "PayPal", para o pagamento direto da reserva efetuada (Funcionamento resumido na Figura 4.19).

Figura 4.19: Diagrama de funcionamento da Página de Confirmação de Dados e Pagamento.

A implementação desta interface de pagamentos na plataforma surgiu com a necessidade de automatização do processo de reservas.

Tendo em consideração que a solução não pode ser industrializada sem ter um sistema de pagamento totalmente funcional, foi necessário recorrer a uma funcionalidade do "PayPal" chamada "Sandbox PayPal". Esta funcionalidade permite testar o funcionamento de um sistema de pagamento, recorrendo a contas fictícias de cliente e proprietário do sistema.

No processo de registo automático da compra de determinado artigo é essencial perceber, no fim da transação, se o pagamento foi feito com sucesso ou não. Para isso, existe uma funcionalidade anexada ao próprio PayPal denominada PDT (*Payment Data Transfer*).

Esta funcionalidade permite a visualização dos detalhes sobre o pagamento efetuado imediatamente após a confirmação da transação por parte do cliente. A Figura 4.20 resume, de certa forma, o funcionamento da funcionalidade PDT no contexto desta dissertação.

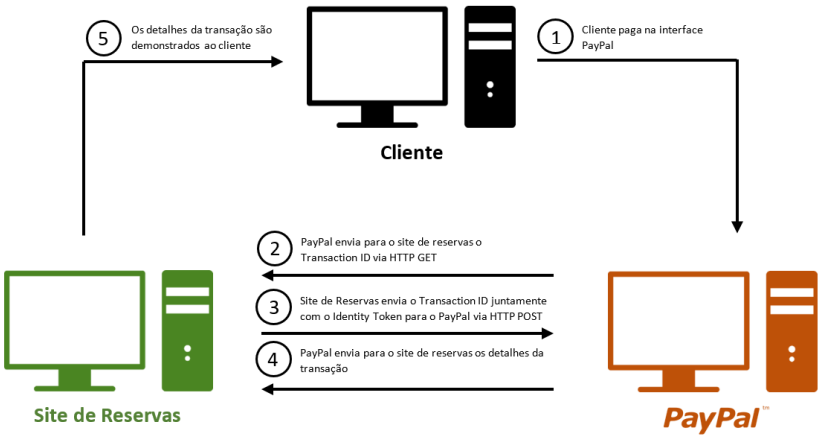


Figura 4.20: Funcionalidade PDT da interface "PayPal" [61]. (Adaptada)

Na Figura 4.20, é possível verificar a presença de três intervenientes no processo de pagamento de determinada compra nesta interface: o Cliente, a Plataforma de Reservas e o próprio "PayPal".

A primeira etapa numa transação via "PayPal", tal como em qualquer outro método de pagamento, reside no pagamento da compra desejada. Após confirmação do pagamento, segue um pedido HTTP GET do "PayPal" para a plataforma de reservas com o *Transaction ID* da compra efetuada. O pedido HTTP encontra-se dividido em duas partes: um URL especificado na conta da plataforma WEB de reservas e o *Transaction ID* anexado ao URL anterior.

Na chegada do *Transaction ID* à plataforma de reservas, é enviado um FORM para o "PayPal" com o *Transaction ID* recebido, juntamente ao *Identity Token* da empresa proprietária da plataforma. Este processo finaliza com uma resposta do "PayPal" ao FORM recebido, a confirmar ou negar o sucesso do pagamento.

Página de Sucesso/Insucesso

Estas páginas foram desenvolvidas com o intuito de confirmar ou negar o sucesso do pagamento da reserva. Na realidade, em termos de ficheiro PHP, estas páginas coexistem no mesmo ficheiro, sendo mostrada uma mensagem de sucesso ou de erro consoante a resposta do "PayPal" ao pagamento feito pelo cliente (Funcionamento resumido na Figura 4.21).

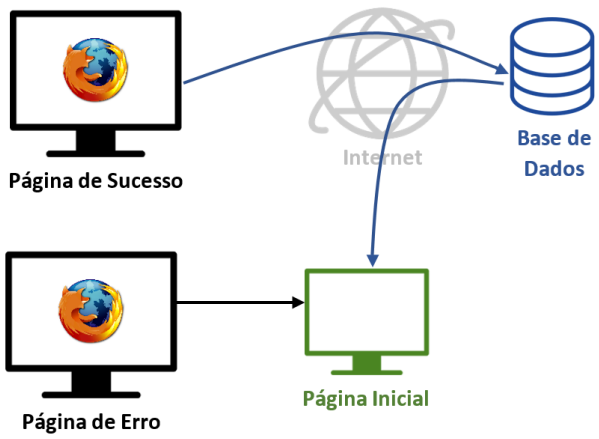


Figura 4.21: Diagrama de funcionamento das Páginas de Sucesso/Insucesso.

A resposta recebida na plataforma de reservas, em relação à confirmação do pagamento da reserva efetuada pelo cliente, contém os campos necessários ao preenchimento da Tabela "Pagamentos" da base de dados do sistema. Essa informação consegue ser retirada do cabeçalho de resposta pela página PHP, utilizando o método GET.

A Figura 4.22 mostra de forma sucinta todo o processo de registo de informação sobre o pagamento através da interface de pagamentos "PayPal" na tabela "Pagamentos" da base de dados do sistema.

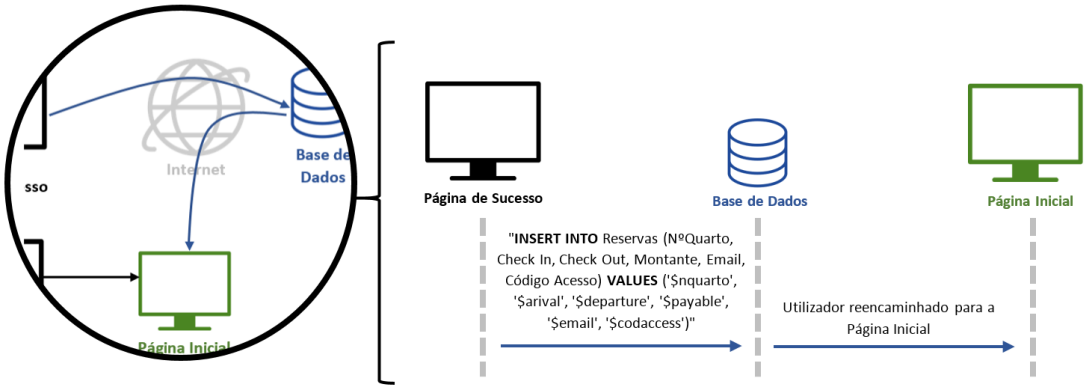


Figura 4.22: Diagrama de interações da comunicação com a BD nas Páginas de Sucesso/Insucesso.

Página de *Login* do Utilizador

A página de *Login* permite a monitorização de alguma informação, segundo o estatuto de cada Utilizador (Cliente ou Administrador). Esta página pode ser acedida através do menu existente na Página Inicial (4.2.2), sendo composta por um pequeno formulário com apenas dois campos - *Email* e *Password* (Funcionamento resumido na Figura 4.23).

Os campos de *login* são definidos de forma diferente para utilizadores com diferentes estatutos. Um utilizador "Cliente" apenas consegue ter credenciais de *login* se fizer alguma reserva na plataforma do sistema. Como já foi referido na secção 4.2.2, existem dois campos no formulário de registo que indicam o *email* e a *password* escolhida pelo cliente. Esses dois campos são relativos às credenciais de *login* do cliente.

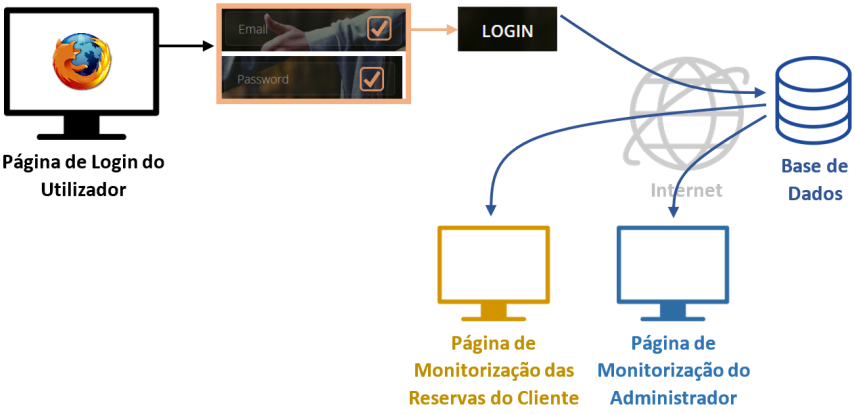


Figura 4.23: Diagrama de funcionamento da Página de *Login*.

Um utilizador "Administrador" não tem oportunidade de escolher as suas credenciais de *login* diretamente na plataforma de reservas. As suas credenciais, por pertencerem a um estatuto de carácter administrativo, são definidas previamente à instalação do sistema na unidade hoteleira. Após submissão dos dados introduzidos, inicia-se mais uma ligação à base de dados do sistema, nomeadamente para a Tabela "Utilizadores".

A comunicação com a base de dados, nesta página, tem o intuito de confirmar as credenciais de *login* introduzidas, bem como associar essas credenciais a um estatuto de utilizador reconhecido pelo sistema (Cliente ou Administrador).

Na eventualidade das credenciais introduzidas serem compatíveis com as registadas na Tabela "Utilizadores", poderão ser apresentadas duas páginas:

- Página de Monitorização para o Administrador
- Página de Monitorização de Reservas para o Cliente

A primeira página, como o nome indica, existe na eventualidade das credenciais introduzidas no formulário de *login* estarem relacionadas com um utilizador "Administrador". Esta página visa apresentar toda a informação relativa às reservas em vigor no sistema, assim como controlar toda a informação dispensada sobre os quartos na plataforma de reservas.

A página de Monitorização de Reservas para o Cliente, por sua vez, foi desenvolvida com a intenção de dar ao cliente oportunidade de conseguir rastrear as suas reservas no sistema.

Na opção de *logout* disponibilizada nas páginas de monitorização, o utilizador é reencaminhado para a página inicial da plataforma de reservas. A Figura 4.24 procura ilustrar as interações entre as páginas de *login*, de Monitorização e entre a base de dados do sistema.

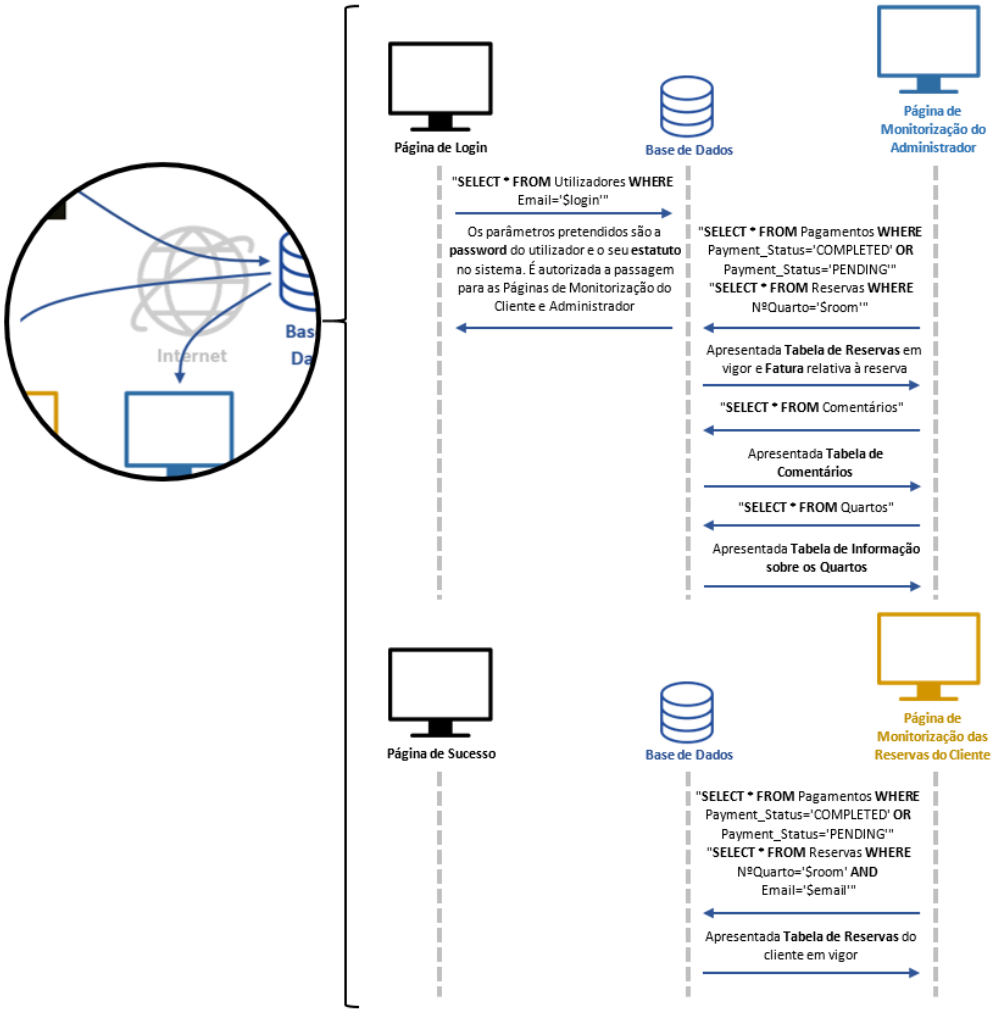


Figura 4.24: Diagrama de interações da comunicação com a BD nas Páginas de *Login* e Monitorização do Administrador e Cliente.

4.2.3 XAMPP - Servidor WEB "Apache"

Como foi referido no início da secção 4.2.2, o *software* XAMPP é constituído por um servidor WEB de acesso livre chamado "Apache".

Um servidor WEB tem como funcionalidade aceitar pedidos HTTP e retornar respostas a esses pedidos. Neste caso, como se trata de um servidor de uma plataforma de reservas, espera-se que os pedidos estejam apenas relacionados com páginas WEB.

O protocolo HTTP define um conjunto de interações entre as aplicações clientes (*Browsers* WEB) e as aplicações servidoras (Servidores WEB). Este protocolo também

define a sintaxe das mensagens enviadas, que todos os clientes e servidores HTTP sabem interpretar.

Para identificar e localizar um documento na Internet, é utilizado o chamado URL (*Uniform Resource Locator*), que mais tarde se passou a chamar URI (*Uniform Resource Identifier*).

Este recurso está essencialmente dividido em 4 partes (Figura 4.25): o protocolo utilizado, o computador de destino, a localização do documento no disco do equipamento de destino e o conjunto variável - valor da variável enviado sobre a forma de *string* para o servidor.

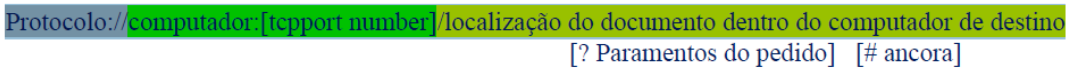


Figura 4.25: Estrutura de um URL.

As interações HTTP presentes na comunicação entre a aplicação de origem e a de destino são do tipo cliente-servidor. Estas interações implicam o envio de uma mensagem HTTP com o pedido do cliente (*Browser* WEB) e uma posterior resposta da aplicação de destino (Servidor WEB). Esta comunicação está dividida em 3 etapas principais:

1. Pedido de Ligação;
2. Envio de mensagem HTTP e respetiva resposta;
3. Fim da Ligação.

Em primeiro lugar, antes de ser enviado um pedido HTTP entre a aplicação cliente e a de destino, a aplicação cliente tem de conseguir estabelecer uma ligação TCP com a aplicação remota (de destino). Através do URL do ficheiro de destino (ex: http://localhost/ficheiro.php), o *browser* WEB fica a saber que deve estabelecer uma ligação TCP com o computador "localhost" e que deve utilizar o protocolo HTTP na interação com a aplicação de destino.

Em segundo lugar, após a ligação TCP estar estabelecida, é necessário enviar uma mensagem HTTP para o equipamento de destino (Servidor WEB). Neste caso, tendo em consideração o URL acima indicado, o *browser* WEB pede ao servidor remoto acesso ao documento "ficheiro.php". Esse pedido segue sob a forma de uma mensagem HTTP do tipo GET.

No fim de receber a mensagem HTTP e processar o seu conteúdo, o servidor WEB gera uma mensagem de resposta começada por "HTTP/1.1 200 OK", acede ao conteúdo do documento "ficheiro.php" e anexa esse conteúdo à mensagem de resposta.

Todo o processo, desde o pedido HTTP até à obtenção da resposta do servido WEB remoto, encontra-se representado na Figura 4.26.

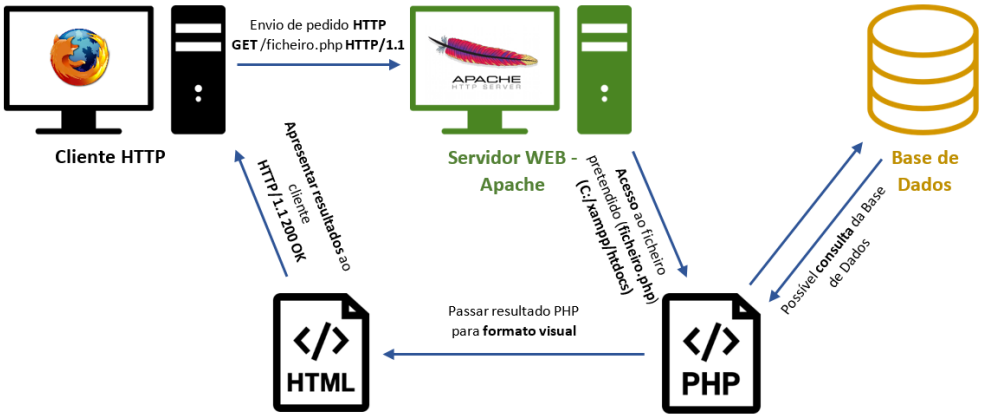


Figura 4.26: Imagem Representativa do processo de envio e resposta a um pedido HTTP.

Por último, após a troca de mensagens necessárias entre o *browser* e o servidor WEB, ambas as aplicações de cliente e de destino encerram a sua ligação TCP.

Existem três tipos de pedidos para o servidor:

- GET: Estas mensagens levam o servidor a responder com informações sobre o documento pedido, incluindo o seu conteúdo;
- HEAD: Este pedido tem o objetivo de pedir apenas informações sobre um documento, como, por exemplo, verificar a sua existência no servidor;
- POST: As mensagens do tipo POST visam atualizar a informação de um documento, anexando ao pedido os novos dados a alterar.

Como referido anteriormente, nesta dissertação foi utilizado um servidor WEB de acesso livre denominado "Apache".

Por defeito, este servidor encontra-se configurado para aceitar ligações através da porta 80. Posteriormente, os pedidos de acesso à base de dados MySQL são reencaminhados para a porta 3306.

As páginas WEB desenvolvidas para a plataforma de reservas (PHP e HTML) são obrigatoriamente armazenadas na pasta C:/xampp/htdocs, presente na raiz do computador, de maneira a estarem acessíveis para posterior consulta.

4.2.4 XAMPP - Servidor de *Emails* "Mercury"

No seguimento do pagamento da reserva e receção da sua respetiva confirmação, é necessário entrar em contacto com o cliente. Este contacto tem por objetivo atribuir um código de acesso ao quarto/alojamento desejado pelo cliente no momento da reserva. Para além do código, este contacto também pretende transmitir toda a informação relativa à reserva efetuada, bem como as datas de *check-in* e *check-out*, entre as quais o código de acesso se encontra válido.

Visto o objetivo desta solução estar centrado na automatização do sistema de reservas e controlo de acessos de determinada entidade hoteleira, a necessidade de ter um sistema automático de envio de mensagens para o cliente é indispensável. Um sistema de envio de mensagens bastante utilizado no mundo computacional é o conhecido *email*.

Neste sistema de reservas, está previsto o envio de um *email* após receção da confirmação do pagamento de uma reserva. Este *email* contém toda a informação relativa à reserva em questão, juntamente com um código de acesso válido entre as datas de *check-in* e *check-out* predefinidas.

Nesta solução, com vista no aproveitamento de *software* já instalado, recorreu-se a uma funcionalidade do XAMPP denominada "Mercury". Esta funcionalidade tem a particularidade de ser um servidor de *emails* que permite à plataforma de reservas enviar uma mensagem de correio eletrónico quando necessário (neste caso, após a receção da confirmação do pagamento da reserva).

Para o envio de *emails* através da plataforma de reservas, foi utilizada uma função PHP denominada "mail". Esta função redireciona todos os pedidos de envio de *emails* para o servidor "Mercury".

Estando o servidor de *emails* "*online*", resta apenas chamar a função"mail" numa página PHP, para poder desfrutar de um sistema de envio automático de *emails* (Funcionamento resumido na Figura 4.27).

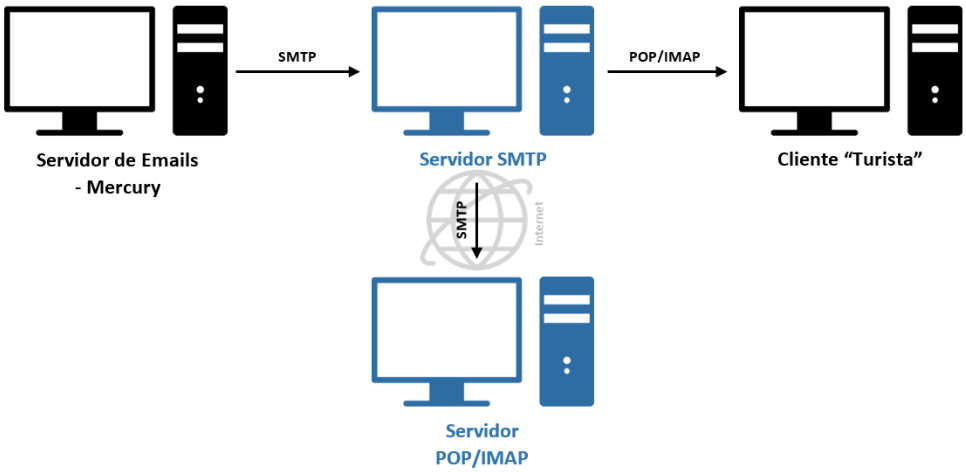


Figura 4.27: Esquema ilustrativo do envio de um *email* através do servidor "Mercury" [62]. (Adaptada)

A configuração do servidor de *emails* "Mercury" encontra-se explicada em detalhe no Apêndice B.

4.2.5 Módulos de Comunicação da Fechadura

Visto o objetivo desta dissertação estar também assente na automatização do controlo de acessos, é fundamental o desenvolvimento de uma fechadura "inteligente". Essa fechadura tem de conseguir, consoante a data de acesso, saber qual o código válido nesse momento, que permite aceder ao espaço pretendido.

O sistema desenvolvido para controlar o acesso ao espaço foi pensado tendo em atenção o custo do *hardware* necessário e a fiabilidade que oferece perante a função a desempenhar.

Sabendo que todos os dados necessários ao bom funcionamento do sistema estão armazenados numa base de dados remota, é fundamental garantir que a fechadura tem

a capacidade de se conectar à rede Internet.

Como foi referido na secção 4.1.3, a comunicação prevista entre a fechadura da solução e a base de dados do sistema pode ser garantida através de duas formas distintas: através do protocolo Wi-Fi ou através dos protocolos GSM/GPRS das comunicações móveis.

Com vista à utilização destes dois protocolos, foram postos à prova dois microcontroladores: SIM900 SHIELD GSM (GSM/GPRS) e NodeMCU v0.9 com ESP8266-12(Wi-Fi).

SIM900 GSM Shield

A primeira opção estudada para comunicação com uma base de dados foi uma *shield* GSM/GPRS (Ver Figura 4.28), que permite o acesso à Internet através do envio de pacotes de dados. A vantagem saliente na utilização deste *modem* assenta no investimento que se consegue poupar na instalação de *routers*/*access points* em locais não preparados para o efeito. Outra vantagem a não esquecer consiste na robustez do acesso à Internet, por não depender de um equipamento terceiro para tal.

A interação com este módulo é feita exclusivamente com recurso a uma série de códigos específicos, denominados "Comandos AT". Uma desvantagem deste módulo reside na utilização deste tipo de comandos como "linguagem de programação". Na eventualidade dos Comandos AT serem enviados numa cadência diferente da "pretendida", o módulo pode não conseguir processar o comando e mostrar uma mensagem de erro. O "Grafcet" da comunicação com o SIM900 encontra-se no Apêndice E.

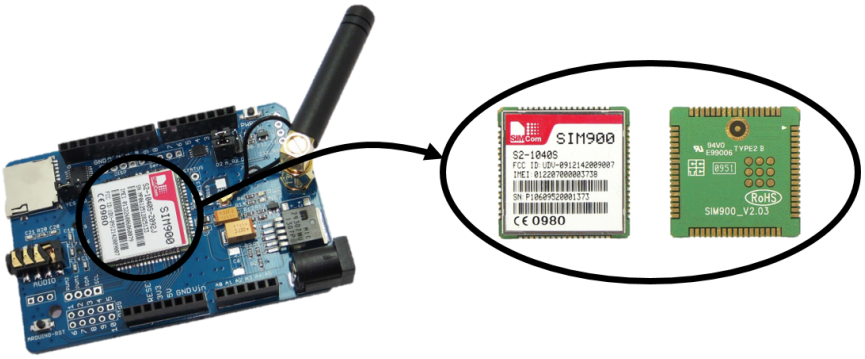


Figura 4.28: Módulo SIM900 [63][64]. (Adaptada)

Inicialmente, antes da escolha do equipamento ideal para a solução defendida nesta dissertação, foi estudada a comunicação entre este módulo e uma base de dados remota.

Nesta situação, tal como na plataforma de reservas, foi utilizado o servidor WEB do XAMPP, denominado "Apache". Este servidor encontra-se originalmente configurado para aceitar ligações na porta 80, sendo que redireciona posteriormente os pedidos de ligação à base de dados para a porta 3306 (MySQL *Server*).

Em primeiro lugar, previamente à comunicação entre o módulo GSM/GPRS e a base de dados do sistema, é necessário iniciar uma ligação TCP entre este módulo e o servidor WEB remoto.

O acesso à base de dados do sistema é garantido através do acesso a ficheiros PHP presentes na pasta C:/xampp/htdocs.

Nesses ficheiros PHP é que se encontra toda a ligação à base de dados. O acesso à informação pretendida é assegurado através do envio, nos ficheiros PHP, de *queries* SELECT, sendo que a inserção de informação pode ser feita com o auxílio de *queries* UPDATE e INSERT (Ver Figura 4.29).

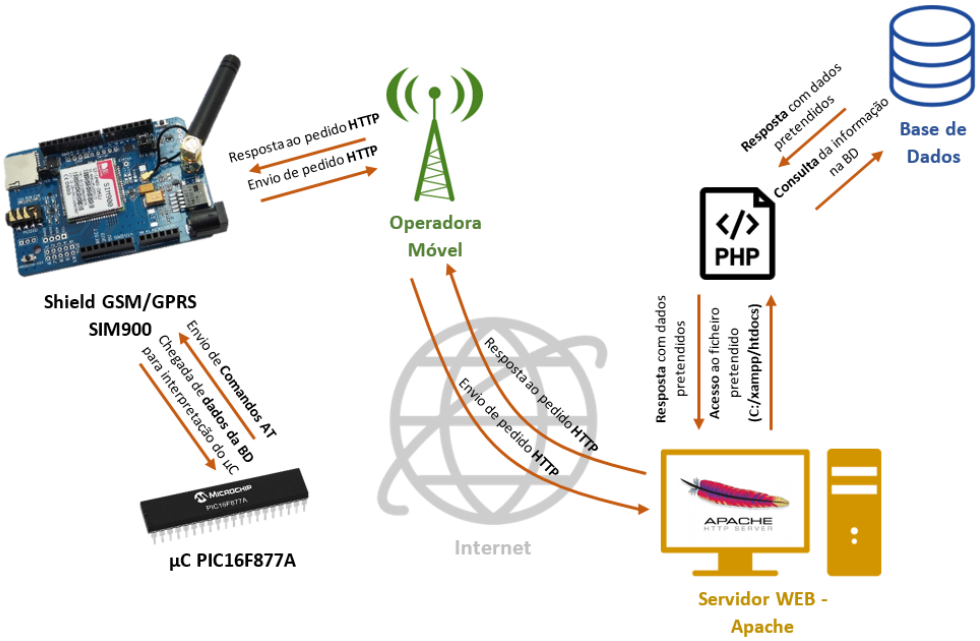


Figura 4.29: Pedido HTTP para a Base de Dados [65]. (Adaptada)

Para o exemplo testado nesta secção, o objetivo da comunicação entre o módulo SIM900 e a base dados consiste na atualização do estado de uns LED's consoante o valor presente numa tabela da base de dados, bem como na atualização do valor de um botão (consoante esteja pressionado ou não) na mesma tabela da base de dados. Tendo em consideração as premissas impostas, apenas serão utilizadas, respetivamente, *queries* de SELECT e UPDATE.

Toda a simulação da montagem elétrica foi feita com o auxílio do programa ISIS.

Para caso de teste, foi utilizado, em ambiente simulado, um microcontrolador PIC16F877A, para controlo dos LED's e do envio das mensagens para o SIM900. O esquema do circuito para comunicação entre o microcontrolador e o SIM900 pode ser consultado no Apêndice F.

A comunicação entre o microcontrolador e o modem é feita através de sinais TTL, sendo que o *modem* consegue reconhecer qual o *baudrate* utilizado na comunicação. Neste caso, o *baudrate* utilizado foi de 19200 bits/s.

Segundo o manual do SIM900, as mensagens enviadas do microcontrolador para o *modem* têm de ser seguidas por um "<CR>"(*Carriage Return*), sendo que as respostas necessitam ter o seguinte formato: "<CR><LF><resposta><CR><LF>" [66].

Alguns dos comandos utilizados no desenvolvimento de uma solução de comunicação entre um módulo SIM900 e uma base de dados estão apresentados na Tabela D.1 do Apêndice D [67].

Inicialmente, ao testar a ligação TCP entre o *modem* e o servidor remoto, foram

encontradas algumas dificuldades devido a bloqueios de segurança na rede da UA (Universidade de Aveiro). Estes bloqueios não permitem a passagem de pedidos de ligação externos a determinado computador ligado à rede da UA. Este problema foi posteriormente resolvido com a instalação de um computador servidor no DEM (Departamento de Engenharia Mecânica), com um endereço IP Público que permite acesso remoto através de outro equipamento.

Na ausência do computador servidor, todos os testes de ligação TCP foram feitos em ambiente doméstico com auxílio de um *router/access point* ligado à rede Internet.

A vantagem de trabalhar numa rede doméstica reside na possibilidade de configurar o *router* para aceitar todos os pedidos de ligação que chegam através de determinada porta e reencaminhá-los para um ou vários equipamentos à escolha. Essa configuração torna possível, por exemplo, a comunicação entre o módulo SIM900 e um computador presente na rede doméstica.

Para existir comunicação entre estes dois dispositivos, é necessário garantir que o computador da rede doméstica tem instalado um servidor WEB que lhe permite aceitar e interpretar pedidos HTTP e enviar a respetiva resposta. Com vista ao aproveitamento de recursos, foi utilizado, à semelhança da plataforma de reservas, o servidor WEB "Apache". Este servidor está configurado para aceitar pedidos de ligação pela porta 80 e, posteriormente, redirecionar os pedidos de acesso à informação da base de dados para a porta 3306 (Todo este processo encontra-se disponível com mais detalhe no Apêndice C).

A comunicação entre o microcontrolador PIC16F877A e o módulo SIM900 é feita exclusivamente através da utilização de comandos AT. A Figura 4.30 demonstra o diagrama de interações seguido no envio dos comandos para o módulo SIM900.

Tendo em consideração a imagem acima, é possível verificar que a ligação TCP entre o módulo SIM900 e o servidor remoto (computador da rede doméstica) apenas é iniciada no comando AT+CIPSTART. Este comando pede o preenchimento de 3 campos: "Tipo de Ligação", "IP Público do Servidor Remoto" e "Porta de Comunicação". O objetivo desta ligação TCP entre os dois equipamentos assenta no acesso a um ficheiro guardado na pasta C:/xampp/htdocs para leitura e atualização de determinada informação na base de dados.

Após o envio do comando AT+CIPSEND, o *modem* responde com o sinal <, indicando ao microcontrolador o momento certo para envio do pedido. O pedido, neste caso, é constituído apenas pelo URL do ficheiro desejado. Sendo pretendida a atualização e o acesso a determinada informação da base de dados, o URL do ficheiro tem de ter anexada a informação que se pretende atualizar (neste caso, o valor do botão).

Esse conteúdo é posteriormente interpretado pelo ficheiro PHP, segundo o método POST, e enviado para a base de dados do sistema, com auxílio de uma *query* UPDATE. Terminada a atualização dos dados, a página PHP envia uma segunda *query* para a base de dados, com o intuito de saber quais os valores dos LED's registados num determinado momento.

A resposta enviada para o módulo SIM900 é composta por 3 números relativos ao estado dos 3 LED's. Esses valores, depois de interpretados pelo programa do microcontrolador, permitem acender ou apagar três LED's específicos da simulação.

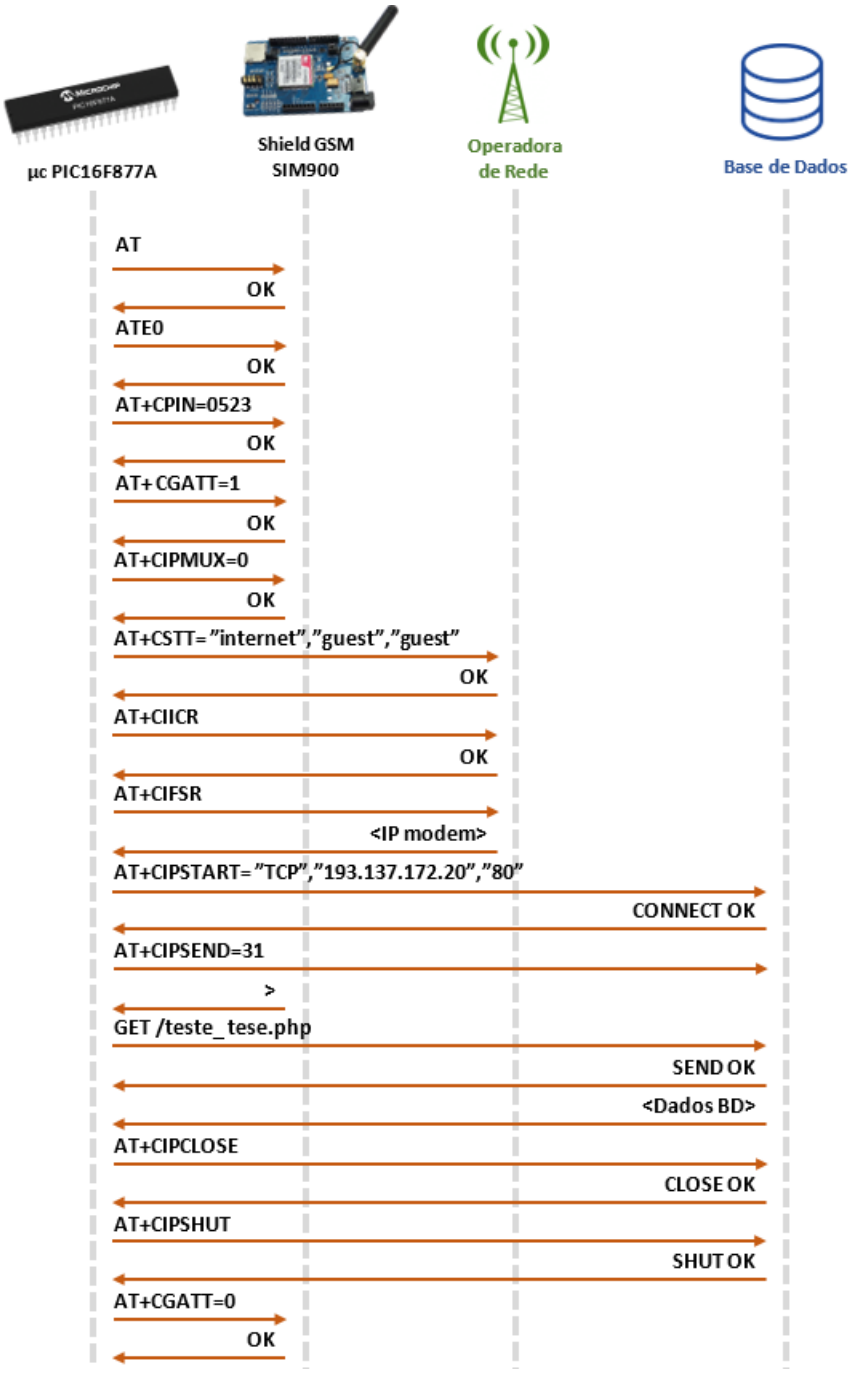


Figura 4.30: Diagrama de interações SIM900.

NodeMCU v0.9 com ESP8266-12

Nesta secção, é proposta uma segunda solução para a comunicação entre a fechadura do alojamento e a base de dados do sistema.

Nesta solução, o acesso da fechadura à rede Internet é conseguido com o auxílio de um módulo NodeMCU (Figura 4.32) e de um *router*/*access point*. Esta solução tem prevista a utilização de um microcontrolador com uma *shield* Wi-Fi, denominado ESP8266-12, para a aquisição da informação necessária para o funcionamento da fechadura.

O NodeMCU, referido anteriormente, consiste numa placa de desenvolvimento constituída por um microcontrolador ESP8266-12 e por uma quantidade significativa de GPIO's (*General Purpose Input/Output*).

Tendo em consideração que o acesso à Internet não se consegue exclusivamente com a utilização deste módulo, é indispensável a aquisição de *routers*/*access points* que permitam ligação por Wi-Fi a outros equipamentos, bem como um acesso suficientemente robusto e rápido à Internet (Ver Figura 4.31).

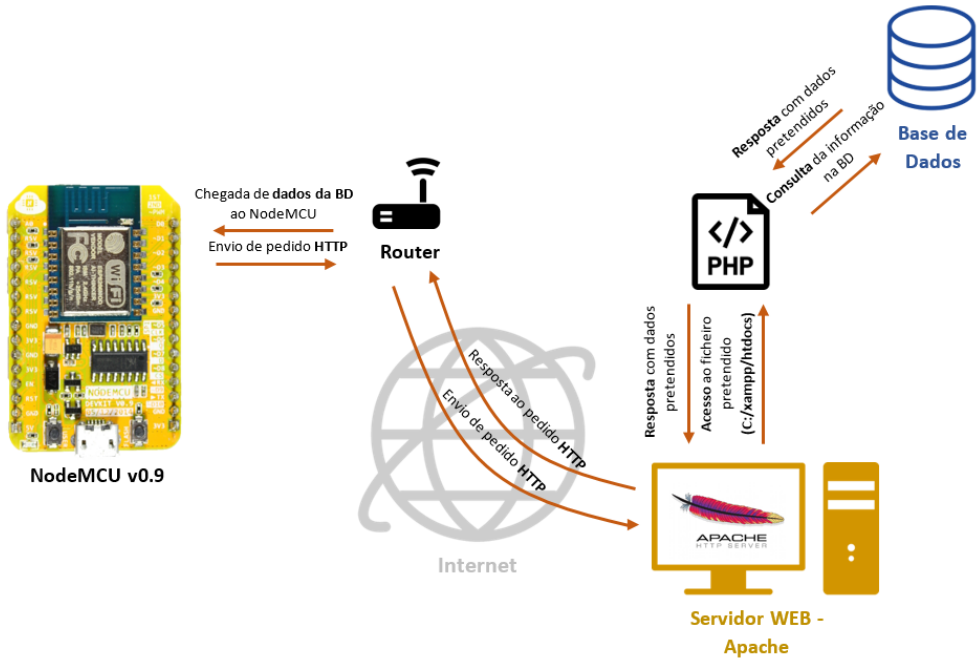


Figura 4.31: Comunicação entre NodeMCU e Base de Dados [68]. (Adaptada)

Uma vantagem saliente na utilização deste equipamento reside na redução de custos na compra de *hardware* (*shield* GSM/GPRS + microcontrolador) para cada fechadura. Outra vantagem importante consiste na poupança mensal em tarifários de rede móvel. É importante salientar que, na solução anterior, a implementação de um módulo SIM900 por fechadura impõe a aquisição de um cartão SIM por módulo. A utilização de um microcontrolador ESP8266-12 (Figura 4.32) traz também vantagens a nível da rapidez de comunicação entre a fechadura e a base de dados do sistema. Esta rapidez permite uma obtenção de dados e registo de informação em tempo "quase" real.

Toda a parte relativa ao programa de controlo da fechadura do sistema e comunicação com a base de dados remota encontra-se alocada no microcontrolador ESP8266. Este

módulo consiste num pequeno *chip* dotado de 2.4GHz Wi-Fi (protocolo IEEE 802.11 com suporte para os protocolos de segurança WPA e WPA2), atualmente muito procurado para aplicações de uso doméstico, pelo seu preço e tamanho bastante reduzidos [69]. Este microcontrolador, com um *firmware* adequado, pode ser programado através de sinais TTL, com auxílio do protocolo de comunicação RS232.

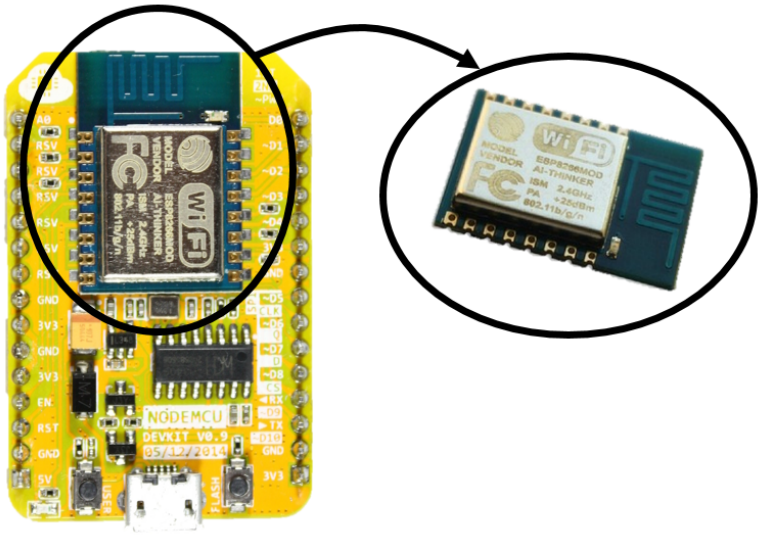


Figura 4.32: NodeMCU (Esquerda); ESP8266-12(Direita) [70]. (Adaptada)

Nesta dissertação, a programação do ESP8266 foi realizada em ambiente Arduino com auxílio do *add-in* do "Visual Studio - Visual Micro". O desenvolvimento de soluções neste tipo de ambiente permite o acesso a determinadas bibliotecas concebidas especialmente para facilitar a vida do programador.

Na Figura 4.33 está representado um fluxograma de funcionamento do programa ESP, para comunicação com a base de dados e posterior controlo de acessos [59].

Tendo por base o Fluxograma apresentado na Figura 4.33, o programa ESP desenvolvido para o controlo de acessos a determinado alojamento é iniciado com a definição de algumas configurações iniciais. Essas configurações encontram-se sub-divididas em:

- Definição de variáveis globais;
- Definição do tipo de pinos utilizados (INPUT ou OUTPUT);
- Estado inicial dos pinos utilizados (HIGH ou LOW).

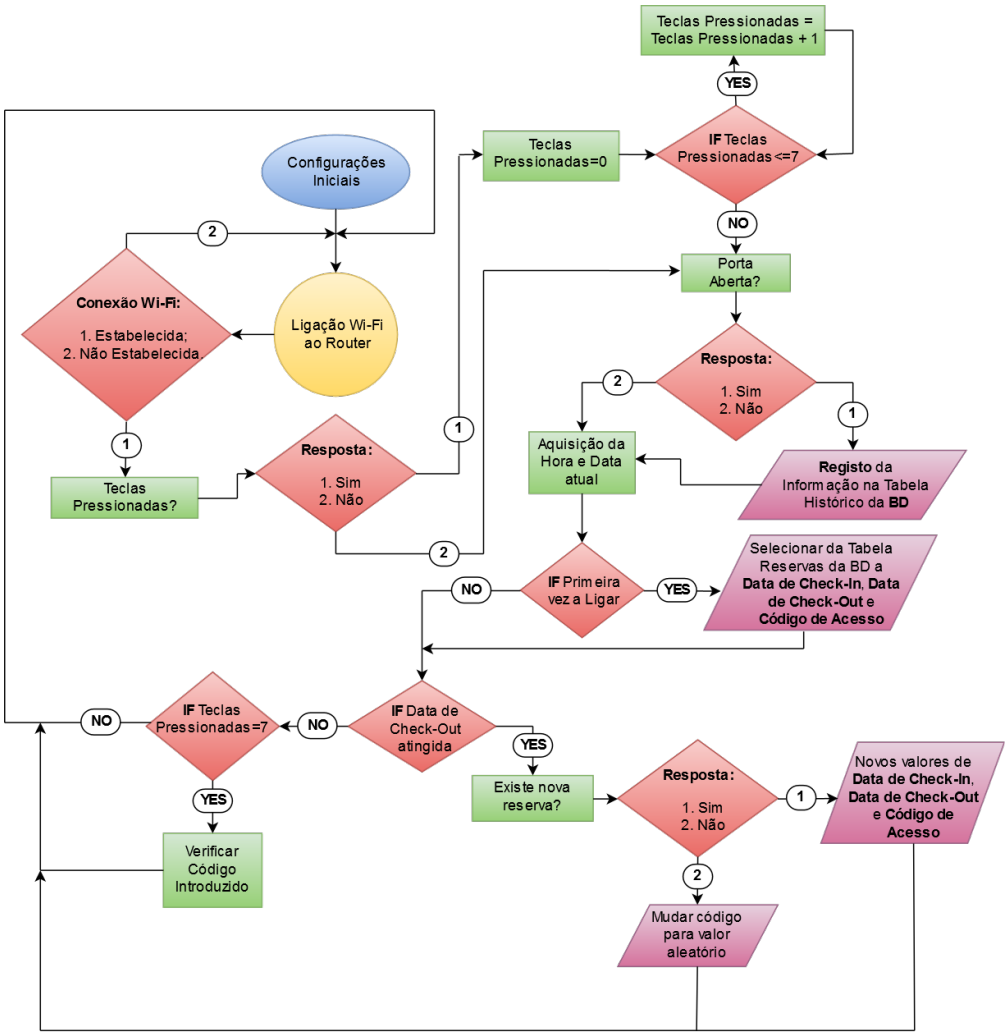


Figura 4.33: Fluxograma de funcionamento da solução com o módulo NodeMCU.

Para a comunicação entre o microcontrolador e o servidor da base de dados do sistema, é necessário garantir o acesso da fechadura à rede Internet. Este acesso é assegurado por uma ligação Wi-Fi entre o microcontrolador e um *router*/*access point* disponível nas suas redondezas. Esta ligação é estabelecida através do processamento de uma rotina que apenas deixa seguir a ordem de comandos do programa depois de assegurar uma ligação Wi-Fi estável entre estes dois equipamentos. Na eventualidade de ocorrer uma falha na comunicação entre o ESP e o *router*, a rotina de ligação Wi-Fi volta ao ativo e apenas deixa continuar o processamento do programa depois de garantir que a ligação se encontra novamente operacional.

O acesso ao alojamento desejado é garantido com a validação de um código de acesso disponibilizado no momento da reserva do cliente. Para identificação das teclas pressionadas, existe uma rotina que, consoante o valor lido na porta analógica, atribui um valor numérico à tecla. De forma a garantir fluidez na leitura das teclas digitadas, ao pressionar a primeira tecla, a rotina entra em *loop* e apenas retorna ao programa depois de pressionar 7 teclas (6 do código e uma de confirmação). Na situação em que o utilizador decide digitar um número de teclas inferior ao pretendido, passado algum tempo,

a rotina encerra e mostra uma mensagem de erro no código. Ao pressionar a 7ª tecla, o programa encerra a rotina de leitura e retorna ao processamento do resto do código.

A verificação do código de acesso digitado também é realizada com recurso a uma rotina no programa ESP. Esta rotina compara o código digitado com o código obtido na comunicação com a base de dados. Consoante a veracidade do código digitado, será concedido ou negado o acesso ao utilizador.

No decorrer do desenvolvimento desta solução, também foi proposta a monitorização da atividade do cliente no alojamento alugado. Esta monitorização está baseada na aquisição do valor de um sensor de abertura da porta. Essa informação é posteriormente armazenada na Tabela "Histórico" da base de dados do sistema, juntamente com a data e hora de abertura.

Numa fase posterior do projeto, esta informação pode ser utilizada, de forma a garantir a limpeza do alojamento numa altura em que o espaço se encontra desocupado.

A aquisição da data e hora do servidor da base de dados é fundamental na gestão das reservas em vigor. Ao atingir a data de *check-out* da sua reserva, o cliente "Turista" perde o direito de acesso ao quarto alugado. Por essa razão, no ESP existe uma rotina que faz a comparação entre a data do servidor e a data de *check-Out* do sistema, para, assim, determinar a mudança do código de acesso válido para o alojamento em questão.

No momento de instalação do sistema, ou numa possível falha de energia no microcontrolador, o programa inicia com a busca da informação à base de dados essencial ao bom funcionamento da fechadura. Essa informação consiste nas datas de *check-in* e *check-out*, bem como no código de acesso ao alojamento pretendido. Tendo a informação atualizada, já é possível prosseguir com o processamento do resto do programa.

Face às vantagens apresentadas na utilização deste tipo de microcontrolador e respetiva placa de desenvolvimento, a sua implementação na solução final para controlo de acessos parece a mais adequada. A velocidade de comunicação com a base de dados do sistema, bem como o processamento da informação recebida são conseguidos apenas com recurso a um equipamento, que tem integrado um microcontrolador ESP8266-12 e uma *shield* Wi-Fi. O preço reduzido do *modem* NodeMCU, aliado às características apresentadas na frase anterior, permite obter uma solução bastante compacta e com a fiabilidade necessária.

4.3 *Hardware*

A obtenção de um sistema de controlo de acessos, para além do desenvolvimento da parte de *software*, também requer a aquisição de *hardware* específico para construção de um protótipo físico.

Os componentes de maior relevância utilizados na construção deste protótipo são:

- Placa de desenvolvimento NodeMCU;
- Teclado Alfanumérico 4x4;
- Fecho elétrico;
- Placas PCB (*Printed Circuit Board*).

As secções seguintes procuram apresentar os componentes acima descritos, juntamente com algumas das suas características mais relevantes. No desenvolvimento do modelo físico final, é necessário ter em consideração alguns aspetos essenciais, que tornam o produto apresentado apetecível em relação a outros presentes no mercado:

- Capacidade de implementação em estruturas já existentes;
- Robustez do produto final;
- Dimensões do sistema a implementar.

É importante relembrar que este projeto ainda está em fase de protótipo, sendo necessária a implementação de alguns ajustes posteriores para o seu lançamento final no mercado.

4.3.1 NodeMCU v0.9

Nesta dissertação, o controlo da fechadura do sistema de controlo de acessos é conseguido com o auxílio da placa de desenvolvimento NodeMCU. Este equipamento apresenta algumas características que permitem diferenciá-lo face a outros módulos semelhantes existentes no mercado.

Esta placa tem como principal constituinte o microcontrolador ESP8266-12, que permite o armazenamento do programa desenvolvido para o controlo da fechadura. As Figuras 4.34 e 4.35 procuram apresentar o "mapa de pinos" do NodeMCU e do respetivo microcontrolador ESP8266-12.

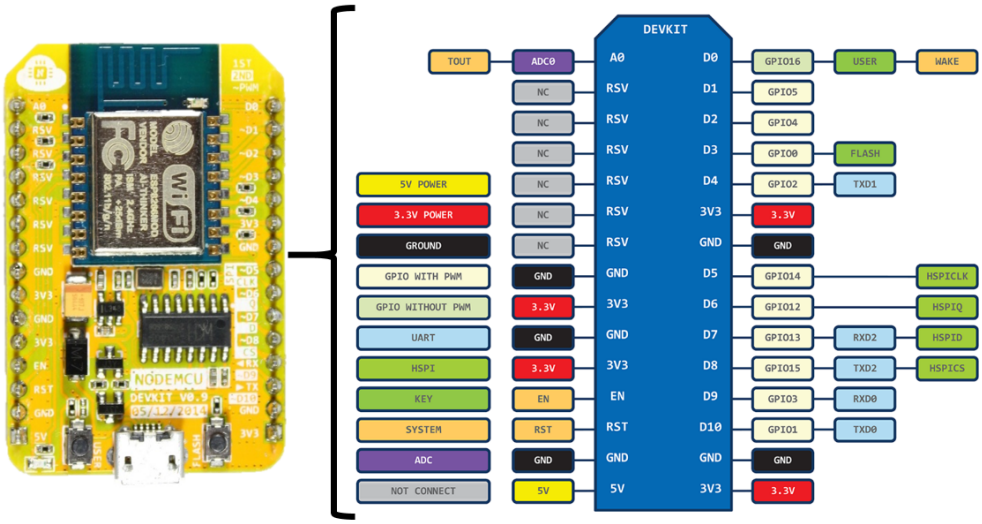


Figura 4.34: Pinos do NodeMCU v0.9 [71]. (Adaptada)

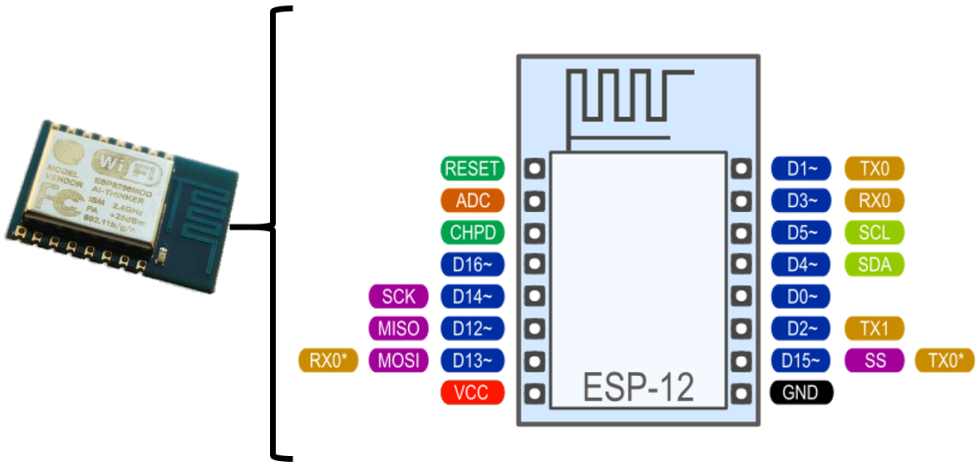


Figura 4.35: Pinos do ESP8266-12 [72]. (Adaptada)

A comunicação entre a fechadura e o *router* mais próximo é assegurada por uma *shield* Wi-Fi embutida nesse mesmo microcontrolador.

O ESP266 contém uma série de especificações técnicas importantes na altura da escolha do equipamento mais adequado à situação em questão. Algumas dessas especificações são [73]:

- 32-bit RISC CPU: Tensilica Xtensa L106 de 80 MHz;
- 64 KB de RAM para instruções, 96 KB de RAM para dados;
- Flash QSPI externa: de 512 KB a 4 MB;
- IEEE 802.11 b/g/n Wi-Fi 2.4 GHz (suporta WEP ou WPA/WPA2);
- 16 pinos GPIO;
- SPI;
- I2C;
- I2S;
- ADC de 10-bit.

A programação do NodeMCU para controlo da fechadura é realizada com auxílio de uma interface micro-USB embutida diretamente na placa de desenvolvimento. A troca de informação entre os dois equipamentos é posteriormente conseguida com a ajuda de um conversor USB-Serial [72].

A porta micro-USB também permite a alimentação da placa com 5V (quando ligada a uma porta USB do computador). Para reduzir e estabilizar a tensão de entrada, o NodeMCU vem agregado com um regulador de tensão que converte os 5V da alimentação em 3.3V. Esta última tensão pode ser utilizada pelos pinos da placa para interagir com outros componentes utilizados na montagem do modelo físico.

Para efeitos de projeto, a placa de desenvolvimento NodeMCU foi utilizada para:

- Controlo de LED's (Vermelho - Código Errado, Verde - Código Certo, Amarelo - Indicador de Tecla pressionada);
- Controlo de abertura e fecho da fechadura (com recurso a uma placa de relés opto-isolados);
- Leitura de Teclas Pressionadas;
- Leitura de Valor do Sensor de abertura da porta.

A Figura 4.36 procura ilustrar a ligação entre o ESP e os componentes acima apresentados.

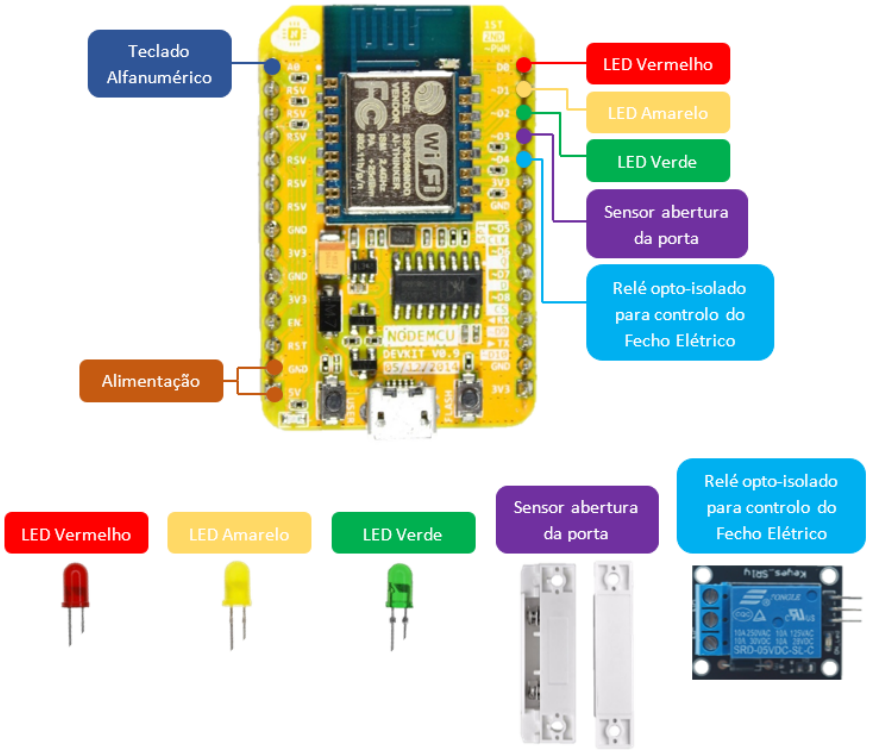


Figura 4.36: Esquema da ligação entre ESP e componentes [74][75]. (Adaptada)

4.3.2 Teclado Alfanumérico 4x4

O sistema de controlo de acessos utilizado nesta dissertação tem por base a utilização de um teclado alfanumérico e a posterior validação do código pelo microcontrolador. A escolha do teclado utilizado teve em conta dois fatores: o preço e a facilidade de implementação (Número de pinos utilizados e Programação da leitura de teclas pressionadas).

De seguida, encontram-se listadas algumas especificações sobre o teclado utilizado:

- Teclado ultra-fino;
- Possível utilização com qualquer microcontrolador;

- Máximos: 24 VDC, 30 mA;
- Interface: 8 pinos resultantes da matriz 4x4;

O teclado encontra-se dividido segundo uma matriz 4x4, em que cada tecla está associada a uma linha e uma coluna (Ver Figura 4.37). Esta disposição tem por objetivo facilitar a interpretação das teclas pressionadas.

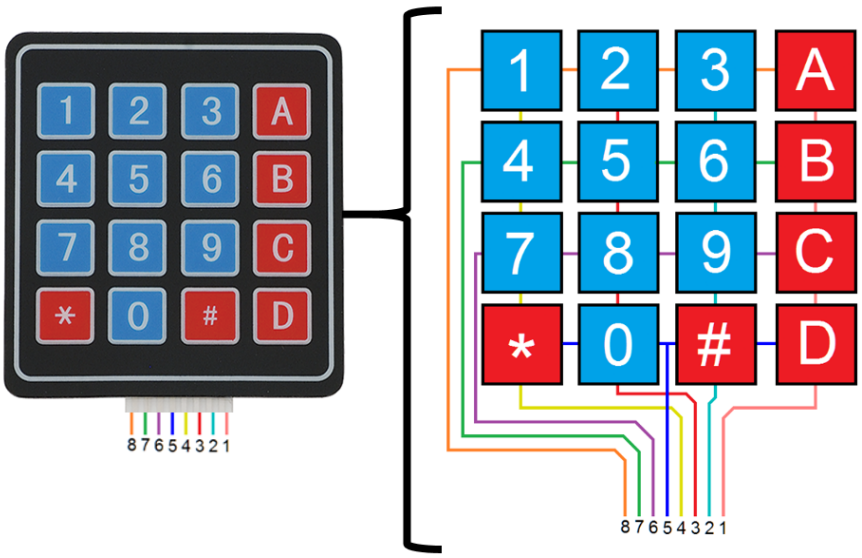


Figura 4.37: Matriz de funcionamento do teclado [76]. (Adaptada)

Tendo em consideração o número de GPIO's da placa de desenvolvimento, a quantidade de pinos utilizados pelo teclado alfanumérico vem restringir o número de componentes possíveis de controlar pelo microcontrolador. Sabendo que a matriz 4x4 dá resultado a um conector com 8 pinos, restam apenas 3 pinos do microcontrolador para controlo de 3 LED's, um sensor de abertura da porta e um fecho elétrico.

A solução adotada nesta dissertação para a redução de pinos utilizados pelo teclado no microcontrolador consiste em utilizar, para a leitura das teclas pressionadas, a entrada Analógica da placa NodeMCU. Os valores analógicos de tensão gerados pelo pressionar de teclas são convertidos em valores ADC pelo conversor Analógico-Digital presente na placa.

A diferenciação entre as teclas é conseguida com auxílio de um conjunto de divisores resistivos aplicados entre cada coluna ou linha da matriz do teclado. Este processo encontra-se explicado com maior detalhe no Apêndice G.

Na Figura 4.38 é possível visualizar a conexão entre o módulo NodeMCU e o Teclado Alfanumérico.

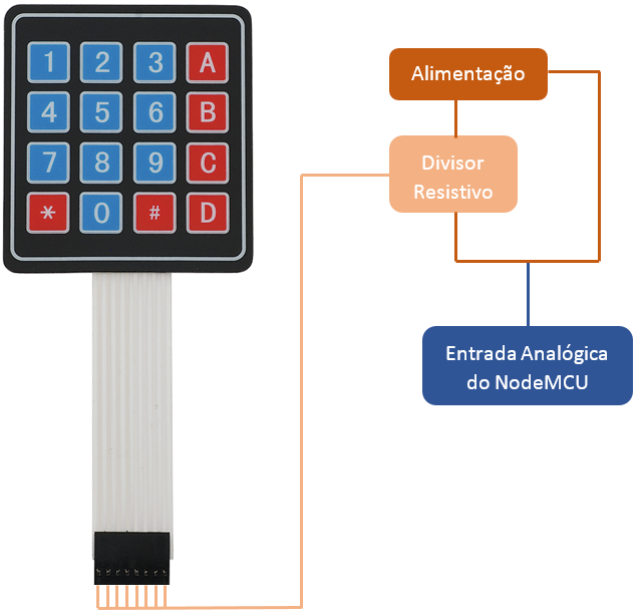


Figura 4.38: Esquema de ligação do Teclado ao NodeMCU.

4.3.3 Fecho Elétrico

Um dos principais objetivos tidos em conta na implementação da solução de controlo de acessos apresentada neste documento é o de desenvolver um sistema capaz de se adaptar às condições oferecidas pela unidade hoteleira. Esta premissa impõe a proposta de uma solução com o menor custo de implementação possível.

De maneira a poder utilizar as mesmas fechaduras já instaladas na unidade hoteleira, a mudança de uma testa da fechadura para um fecho elétrico de batente parece ser a solução mais viável de implementar (Ver Figura 4.39).

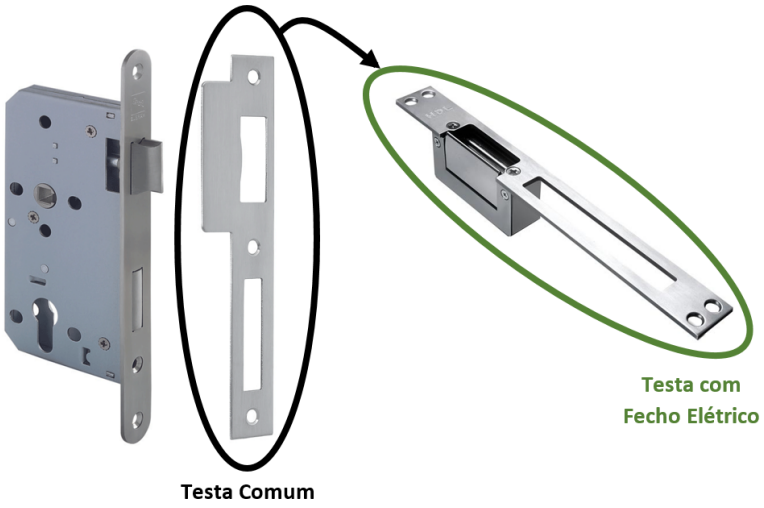


Figura 4.39: Testa com Fecho Elétrico de batente.

A interface entre o *modem* NodeMCU e a fechadura é feita com auxílio de um relé opto-isolado que de um lado é atracado com os 3.3V da saída digital do microcontrolador e do outro permite a alimentação da fechadura com os 12V necessários. A parte opto-isolada existe para proteção da placa, evitando que um possível curto-circuito, ou qualquer outra falha elétrica proveniente da fechadura, danifique os componentes existentes do lado do microcontrolador.

A Figura 4.40 procura ilustrar a ligação entre a fechadura e o *modem* NodeMCU.

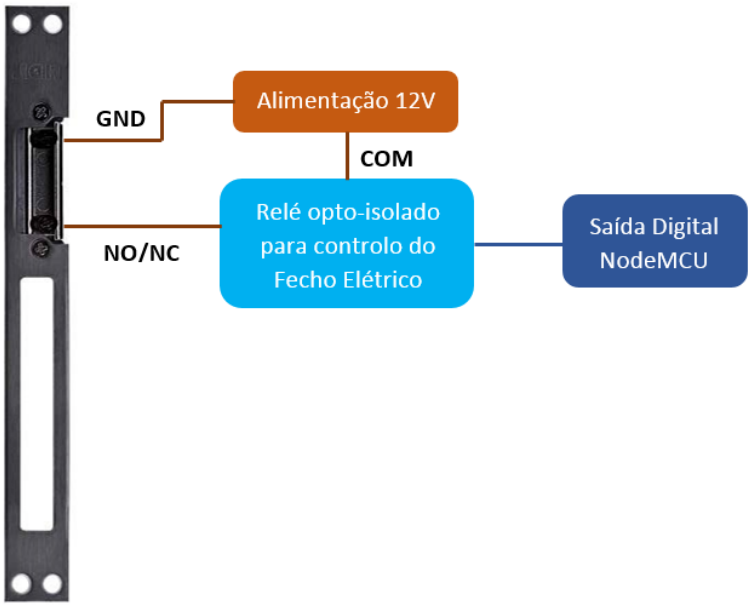


Figura 4.40: Esquema de ligação da fechadura ao NodeMCU.

4.3.4 Placas PCB

Para complemento desta dissertação, e de modo a aproximar a solução apresentada de um protótipo final, foram desenvolvidas e impressas umas placas de circuito impresso (PCB). Estas placas foram desenvolvidas com o auxílio do *software* "Eagle" da "AutoDesk". Este *software* permite a utilização de uma biblioteca com uma vasta lista de componentes, de modo a facilitar a modelação das placas desejadas.

Para esta dissertação, foram desenvolvidas duas placas:

- Placa para implementação do Teclado (Figura 4.41);
- Placa para alimentação e controlo da Fechadura (Figura 4.42).

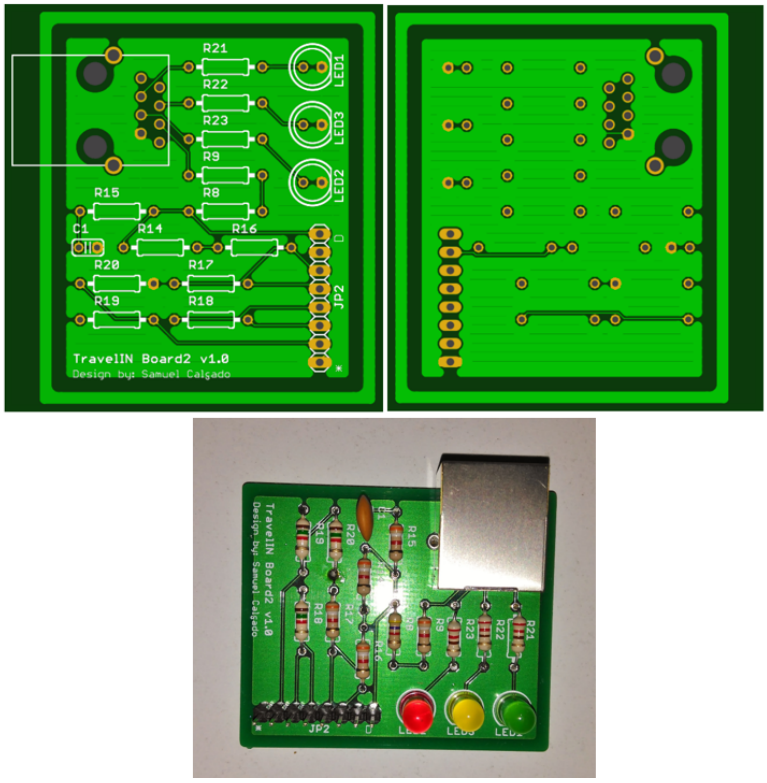


Figura 4.41: Placa para implementação do Teclado.

A divisão da montagem em duas placas acontece somente por razões de segurança. A necessidade de ter toda a parte de alimentação do sistema no interior do alojamento garante a impossibilidade de acesso aos cabos de 12V do fecho elétrico. Essa premissa existe com o intuito de garantir a segurança do utilizador do espaço. A instalação da placa do teclado no exterior da porta acontece devido à obrigação de ter o teclado alfanumérico instalado num local acessível aos utilizadores do alojamento.

A ligação entre as duas placas é conseguida com a utilização de um cabo "Ethernet". Este cabo permite a passagem da alimentação para a placa do teclado, assim como todos os cabos do teclado, para posterior leitura das teclas.

A placa de alimentação, para além dos 12V fornecidos diretamente pela unidade hoteleira, também possui uma bateria de segurança que pode ser utilizada em caso de falha de corrente. Esta solução assemelha-se ao funcionamento de uma UPS (*Uninterruptible Power Supply*) e permite o carregamento da bateria em paralelo à alimentação do sistema. No caso de uma falha de energia, o funcionamento do sistema de controlo de acessos é apenas assegurado pela bateria.

Para evitar sobreaquecimentos no NodeMCU e possíveis danos futuros nalguns outros componentes, a alimentação desejada para esta placa de desenvolvimento ronda os 5V. A passagem dos 12V de alimentação direta para os 5V desejados é conseguida com a utilização de um regulador de tensão LM7805 e de um conversor 5VDC-5VDC. Os 12V diretos apenas foram utilizados para alimentação do fecho elétrico e carregamento da bateria.

O circuito das placas pode ser visualizado no Apêndice H.

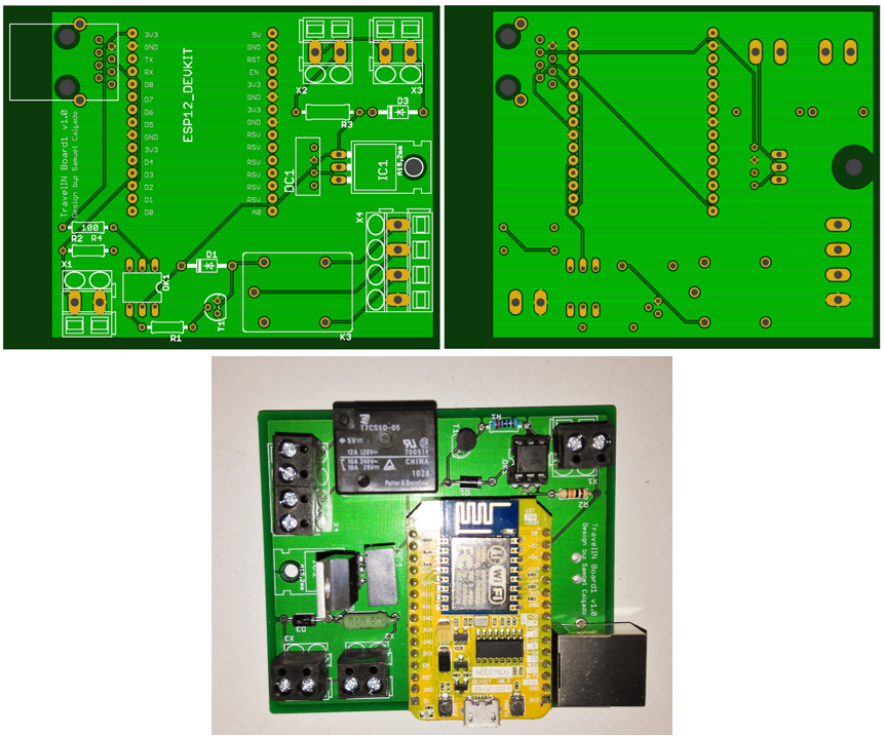


Figura 4.42: Placa para alimentação e controlo da Fechadura.

4.3.5 Montagem Final

Esta secção procura apresentar a montagem final relativa ao sistema de controlo de acessos desenvolvido (Figuras 4.43, 4.44 e 4.45). A alimentação a 12V das placas é conseguida com a utilização de um transformador regular, que converte os 220V da tomada nos 12V desejados.

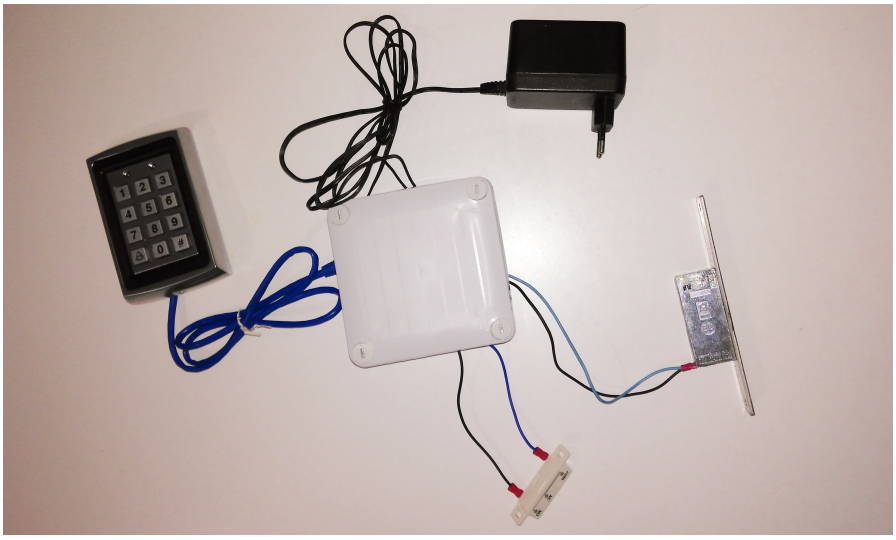


Figura 4.43: Montagem Final - 1.

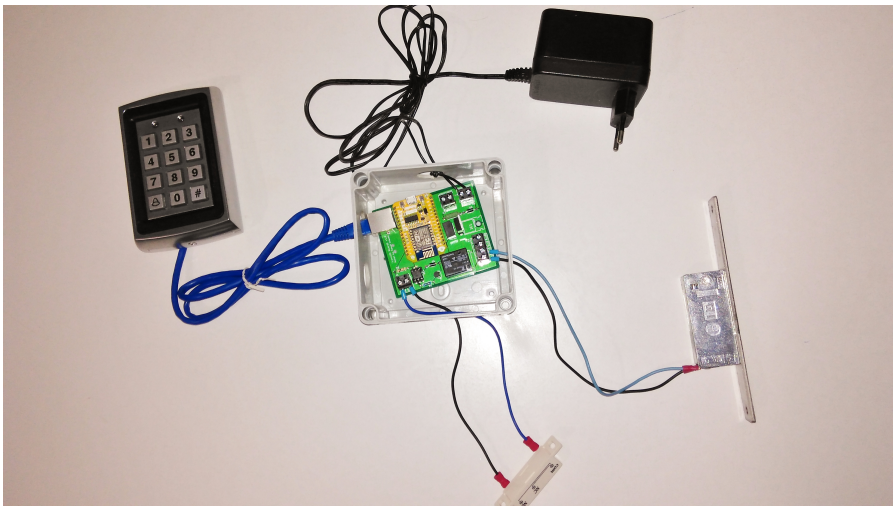


Figura 4.44: Montagem Final - 2.

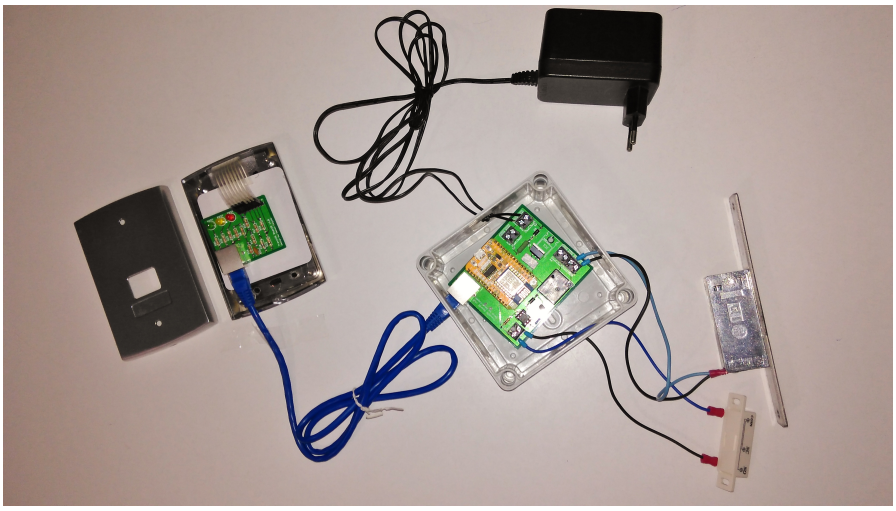


Figura 4.45: Montagem Final - 3.

É importante salientar que o teclado presente nestas imagens não foi o teclado utilizado na simulação e teste da solução (Apenas foi utilizado para aproximar o protótipo apresentado de uma possível solução comercializável).

O custo de aquisição do *hardware* necessário para a montagem final do protótipo, apresentado nesta secção, encontra-se ilustrado na Tabela 4.7. Este parâmetro consiste num dos pontos principais tido em consideração no desenvolvimento desta solução.

Tabela 4.7: Custo aproximado do Protótipo Final.

Nome	**Detalhes**	**Preço**
Placas PCB	As placas PCB foram compradas em lotes de 5. Cada lote custou 10€(com envio incluído).	4€
Transformador 12V	Preço aproximado para 1 unidade.	3€
Trinco Fechadura (Testa)	Preço aproximado para 1 unidade.	10€
Sensor de Abertura	Preço aproximado para 1 unidade.	2€
Teclado de Exterior com Caixa Metálica	Preço aproximado para 1 unidade.	25€
NodeMCU	Preço aproximado para 1 unidade.	3€
Restantes Componentes	Ao serem comprados em grandes lotes, cada unidade de cada componente tem um preço bastante reduzido.	3€
TOTAL		**50€**

Capítulo 5

Considerações Finais

5.1 Conclusões

A automatização de edifícios tem sido um fator de grande discussão ao longo destes últimos anos mas, devido ao preço elevado dos equipamentos necessários e à falta de retorno do investimento, a sua implementação não tem sido tão notória quanto o esperado.

O crescimento sistemático do número de dormidas, tanto a nível nacional como a nível mundial, demonstra a importância do Turismo na balança económica de um dado país.

Sabendo que grande parte das dormidas acontece em unidades hoteleiras, esta dissertação procura apresentar um sistema de reservas e controlo de acessos totalmente automático (sendo a solução mais apelativa para *Guest Houses*, etc. - ambientes mais pequenos). Esta solução prevê a diminuição de custos relacionados com o funcionamento 24/24 horas de uma receção hoteleira, bem como o aumento da comodidade dos utilizadores do sistema (cliente e administrador).

Os mecanismos de controlo de acessos presentes no mercado, apesar de bastantes apelativos e seguros, apresentam algumas desvantagens a nível de custos de implementação e falta de automatização no seu funcionamento. Atualmente, as soluções mais utilizadas na indústria hoteleira são as chaves metálicas (mais comuns), os mecanismos que recorrem a utilização de um teclado numérico e a tecnologia RFID. As chaves metálicas, apesar da sua fiabilidade de utilização, apresentam algumas desvantagens, como:

- Falta de automatização do sistema: É sempre necessário alguém para entregar e recolher as chaves nas datas de *check-in* e *check-out* da reserva;
- Despesas extra com a troca da fechadura se:
  - Cliente ficar com a chave no fim da estadia;
  - Cliente fizer cópia das chaves;
  - Cliente perder as chaves.
- Entre outras, etc.

Os sistemas RFID, apesar de facilitarem o acesso, apresentam desvantagens semelhantes aos sistemas com chave metálica, por recorrerem a uma *tag* de identificação para o acesso ao espaço pretendido. Este sistema também possui um custo de implementação

mais elevado, por necessitar da instalação de um leitor para leitura das *tags* RFID dos clientes.

Existem também outros mecanismos de identificação do utilizador que, apesar da sua elevada segurança no controlo de acesso, não justificam a sua utilização numa unidade hoteleira, por terem um custo de implementação demasiado elevado e necessitarem de um pré-registo da informação do utilizador, considerado excessivamente invasivo (para além de exigir a presença prévia do cliente na unidade hoteleira).

A solução proposta neste documento propõe a utilização de uma plataforma de reservas - para o registo da informação pertinente à reserva numa base de dados remota - e um microcontrolador (com uma *shield Wi-Fi*) na fechadura do alojamento, para comunicação com a base de dados e interpretação dos dados necessários ao seu funcionamento.

Este sistema permite um registo das reservas na base de dados e o envio de um *email* ao cliente com toda a informação relativa à sua reserva de forma totalmente automática, após a confirmação do pagamento. O microcontrolador embutido na fechadura apenas tem a função de saber qual o código de acesso válido para uma reserva em vigor, para determinado alojamento. Os dados necessários ao seu funcionamento são as datas de *check-in* e *check-out*, o código de acesso atribuído à reserva e a data e hora atual para controlo do início e fim da estadia.

Nesta solução, o microcontrolador também envia para a base de dados um histórico de aberturas da porta, para um posterior controlo da atividade do cliente.

O mecanismo de controlo de acessos mais adequado para o sistema em causa, tendo em consideração os objetivos de automatização e o custo de implementação do sistema, consiste numa fechadura com teclado alfanumérico.

O sistema desenvolvido cumpriu com os requisitos de automatização do sistema e baixo custo do *hardware* necessário, tanto para a comunicação com a base de dados, como para o funcionamento da própria fechadura. Um custo que não se teve em consideração no desenvolvimento desta solução e que, possivelmente, consiste na maior despesa na passagem deste protótipo para uma solução comercial, reside na compra de um servidor para alojamento da base de dados do sistema e da própria plataforma de reservas.

Apesar da ausência de uma gama de testes intensivos ao sistema (não foi testado em ambiente real), o seu comportamento a curto prazo demonstrou uma fiabilidade satisfatória, tendo em consideração a fraca aplicabilidade industrial do ESP. A plataforma de reservas, por sua vez, permite a reserva do alojamento pretendido, disponível para as datas de *check-in* e *check-out* desejadas, bem como o seu pagamento através da interface de pagamentos *online* "PayPal". Para teste do sistema de pagamento, foi utilizada uma ferramenta do "PayPal" denominada "SandBox". A passagem do sistema protótipo para uma solução comercial requer alguns ajustes posteriores para o pagamento e consequente transferência do montante da estadia do cliente para o administrador da unidade hoteleira.

Foram realizados alguns testes para a verificação de erros no decorrer da utilização da plataforma, não tendo sido verificada nenhuma discrepância que pusesse em causa a viabilidade da solução apresentada.

5.2 Sugestões de trabalho futuro

Numa perspetiva de continuidade do trabalho desenvolvido, são propostas, nesta secção, algumas sugestões de melhoria para o sistema desenvolvido:

1. **Utilização de um "IO expander" na interface com o Teclado Alfanumérico:** A solução apresentada neste documento utiliza um pequeno divisor resistivo para leitura das teclas pela porta analógica do ESP. Este divisor permite a obtenção de diferentes valores de tensão, consoante a tecla pressionada, sendo esse valor posteriormente interpretado pela ADC do microcontrolador e convertido para um número entre 0 e 1024. A atribuição do valor da tecla é feita por comparação do valor ADC da afinação do sistema com o valor obtido no momento do pressionar da tecla.

   Apesar da margem dada na comparação do valor lido com o valor predefinido na afinação, podem existir erros de leitura causados por pequenas variações de tensão na entrada analógica do ESP.

   Dessa forma, a utilização de um "IO expander" com interface de comunicação I2C, para além do acrescento de GPIO's (8 pinos para o teclado), permite uma leitura mais estável das teclas pressionadas.

2. **Teclado Virtual embutido no ESP:** Uma forma de tornar o sistema proposto mais apelativo e inovador em relação às restantes soluções existentes no mercado consiste na implementação de um teclado virtual no microcontrolador da fechadura.

   Esta solução requer uma pré-configuração do ESP como servidor WEB de uma página PHP/HTML, para *display* do teclado virtual. Para aceder à página, é necessário um equipamento com capacidade de comunicação por Wi-Fi e com um *browser* WEB (para envio do pedido HTTP e posterior visualização da página).

3. **Implementação de sensores**: A atividade do cliente no alojamento pode ser monitorizada com auxílio de uns sensores específicos (temperatura, sensor fotoelétrico, etc.). Esta informação pode ser posteriormente utilizada, para efeitos estatísticos, na gestão do horário de limpezas, ou até mesmo no controlo da entrada de novos clientes (caso o "antigo" cliente ainda se encontre nas instalações, o "novo" cliente não pode entrar no alojamento).

4. **Utilização de outros microcontroladores:** A expansão do sistema proposto nesta dissertação (adição de sensores para monitorização da atividade do cliente), pode levar a uma sobrecarga na capacidade de processamento oferecida pelo ESP.

   Um microcontrolador mais potente garante uma fiabilidade de utilização consideravelmente superior à do ESP e proporciona uma maior fluidez na utilização do sistema.

Bibliografia

[1] Atividade Turística em Junho de 2016. INE (Instituto Nacional de Estatística); 2016.

[2] Gabbai AS. Kevin Ashton Describes The Internet of Things; 2015. [Accessed on: 2017-10-22]. Available from: https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/.

[3] Morgan JCF. Forbes: A Simple Explanation Of The Internet Of Things; 2014. [Accessed on: 2017-10-22]. Available from: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/{#}7307530f1d09.

[4] Kobie NTG. The Guardian: What is the internet of things?; 2015. [Accessed on: 2017-10-22]. Available from: https://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google.

[5] Harris S. CISSP All-in-One Exam Guide. 6th ed. McGraw Hill Professional; 2012. Available from: https://books.google.pt/books?id=vBK2RE{_}h0EUC{&}q=cissp+all+in+one{&}dq=cissp+all+in+one{&}hl=pt-BR{&}sa=X{&}redir{_}esc=y.

[6] Cardoso D. Controlo de acessos no sector turístico [Dissertação de Mestrado]. Universidade de Aveiro; 2015.

[7] Segurança Online: Riscos e Graus de Segurança;. [Accessed on: 2017-10-23]. Available from: http://www.segurancaonline.com/gca/?id=970.

[8] Zúquete ARIdUdA. Segurança em redes informáticas. 4th ed. FCA - Editora de Informática; 2013. Available from: http://ria.ua.pt/handle/10773/15996.

[9] Santos (Universidade de Aveiro) JP. Apontamentos de Informática Industrial, EIA232; 2016.

[10] Valadão RBUEP. Poluição em Redes P2P; 2008. [Accessed on: 2017-10-25]. Available from: https://www.gta.ufrj.br/ensino/eel879/trabalhos{_}vf{_}2008{_}2/renan{_}bernardo/p2p.html.

[11] Wikipedia: Peer-to-Peer;. Available from: https://pt.wikipedia.org/wiki/Peer-to-peer.

[12] Pereira de Oliveira J. Análise de desempenho de TCP sobre GPRS em um ambiente fim a fim [Dissertação de Mestrado]. Universidade Federal de Pernambuco; 2004. Available from: http://repositorio.ufpe.br:8080/xmlui/handle/123456789/2518.

[13] Gruber V. Sistema de Monitoramento com GSM/GPRS [Dissertação de Mestrado]. Universidade Federal do Rio Grande do Sul; 2007. Available from: http://www.lume.ufrgs.br/bitstream/handle/10183/77204/000625552.pdf?sequence=1.

[14] Magno R, Recharte D, Gonçalves D, Ferrão D. Como evoluiram as normas Wi-Fi IEEE 802.11? Faculdade de Engenharia da Universidade do Porto; 2013. Available from: https://paginas.fe.up.pt/{~}projfeup/submit{_}13{_}14/uploads/relat{_}1MIEEC01{_}3.pdf.

[15] Santos JP. Apontamentos de Informática Industrial, TCP/IP. Universidade de Aveiro; 2016.

[16] Finnie SSN. 20 Questions: How the Net Works;. [Accessed on: 2017-10-25]. Available from: http://www.scotsnewsletter.com/20quests/hownet.htm.

[17] Santos JP. Apontamentos sobre Bases de Dados. Universidade de Aveiro; 2016.

[18] Gerard JC. How Does a Keypad Lock Work?;. [Accessed on: 2017-10-23]. Available from: http://smallbusiness.chron.com/keypad-lock-work-36063.html.

[19] Aliexpress: Sistema de controlo de acesso com Teclado e RFID;. [Accessed on: 2017-10-23]. Available from: https://pt.aliexpress.com/store/product/SIB-Keypad-RFID-Access-Control-System-Proximity-Card-Standalone-2000-Users-Door-Access-Control-Metal-Case/204596{_}32761885795.html.

[20] Wikipedia: Barcode;. [Accessed on: 2017-10-23]. Available from: https://en.wikipedia.org/wiki/Barcode.

[21] Wikipedia: Código de Barras EAN-13;. [Accessed on: 2017-10-23]. Available from: https://pt.wikipedia.org/wiki/EAN-13.

[22] Brain MH. How UPC Bar Codes Work; 2000. [Accessed on: 2017-10-23]. Available from: https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/upc.htm.

[23] Wikipedia: QR Codes;. Available from: https://en.wikipedia.org/wiki/QR{_}code.

[24] Pontius NC. Data Matrix Codes vs QR Codes; 2017. [Accessed on: 2017-10-23]. Available from: https://www.camcode.com/asset-tags/barcodes-data-matrix-vs-qr-codes/.

[25] Atteberry JH. How 2-D Bar Codes Work; 2011. [Accessed on: 2017-10-23]. Available from: https://science.howstuffworks.com/innovation/repurposed-inventions/2d-barcodes1.htm.

[26] Wikipedia: PDF417;. Available from: https://en.wikipedia.org/wiki/PDF417.

[27] Condeço G. Tecnologia RFID: Caso de Estudo Aplicado à Logística Hospitalar [Dissertação de Mestrado]. Universidade de Lisboa; 2015. Available from: http://repositorio.ul.pt/bitstream/10451/22958/1/ulfc117340{_}tm{_}Gon{ç}alo{_}Conde{ç}o.pdf.

[28] Sweeney II PJ. RFID for Dummies. Wiley Publishing, Inc; 2010. Available from: https://books.google.pt/books?id=Gb6w54X7Kw0C{&}printsec=frontcover{&}dq=RFID+for+dummies{&}hl=pt-BR{&}sa=X{&}redir{_}esc=y{#}v=onepage{&}q=RFIDfordummies{&}f=false.

[29] Research Design Lab: RFID Reader;. [Accessed on: 2017-10-23]. Available from: https://researchdesignlab.com/iot-enabled-rfid-reader.html.

[30] Skinner NNSb. Building An Active RFID People/Asset Tracking System With Mesh Networking; 2010. [Accessed on: 2017-10-23]. Available from: http://www.ns-tech.co.uk/blog/2010/02/active-rfid-tracking-system/.

[31] Bibi F, Guillaume C, Gontard N, Sorli B. RFID technology having sensing aptitudes for food industry and their contribution to tracking and monitoring of food products. Trends in Food Science & Technology. 2017;62:91–103. Available from: http://www.sciencedirect.com/science/article/pii/S0924224416304198.

[32] CAS Dataloggers: CAEN RT0005 RFID Temperature Logger Semi-Passive UHF Tag;. [Accessed on: 2017-10-23]. Available from: https://www.dataloggerinc.com/product/rt0005-rfid-temperature-logger-semi-passive-uhf-tag/.

[33] NFC Experts: NFC Payment;. [Accessed on: 2017-10-23]. Available from: http://www.nfc-experts.com/nfc-payment.html.

[34] Hamann RT. Governo pretende regulamentar sistemas de pagamento por celular; 2012. [Accessed on: 2017-10-23]. Available from: https://www.tecmundo.com.br/governo/26585-governo-pretende-regulamentar-sistemas-de-pagamento-por-celular.htm.

[35] Irvine C. HID Global: HID Global Completes World's First Series of NFC-Enabled Smartphone Pilots that Open Doors in the Enterprise; 2012. [Accessed on: 2017-10-23]. Available from: https://www.hidglobal.com/press-releases/hid-global-completes-worlds-first-series-nfc-enabled-smartphone-pilots-open-doors-in.

[36] Cervantes EA. How to use NFC on Android; 2017. [Accessed on: 2017-10-23]. Available from: https://www.androidauthority.com/how-to-use-nfc-android-164644/.

[37] Activa ID: Leitor NFC USB ACR122U;. [Accessed on: 2017-10-23]. Available from: http://activa-id.com.br/produto/leitor-nfc-usb-acr122u.

[38] RFID Tags: NFC tags; 2016. [Accessed on: 2017-10-23]. Available from: http://www.cxjrfidfactory.com/tag/nfc-tags/page/3/.

[39] Ozdenizci B, Coskun V, Ok K. Near field communication (NFC) : From Theory to Practice. Wiley Publishing, Inc; 2012. Available from: https://books.google.pt/books?id=-n3DZtCyFl8C{&}printsec=frontcover{&}dq=Near+field+communication+(NFC)+:+From+Theory+to+Practice{&}hl=pt-BR{&}sa=X{&}redir{_}esc=y{#}v=onepage{&}q=Nearfieldcommunication(NFC){%}3AFromTheorytoPractice{&}f=false.

[40] Philips: Near Field Communication;. [Accessed on: 2017-10-24]. Available from: http://www.sacg.com.tw/sacweb/marcom/epaper/images/NFC.pdf.

[41] Poole IRE. NFC Modulation & RF Signal;. [Accessed on: 2017-10-24]. Available from: http://www.radio-electronics.com/info/wireless/nfc/near-field-communications-modulation-rf-signal-interface.php.

[42] Motlagh NH. Near Field Communication (NFC) - A technical Overview [Master of Science Degree]. Aalto University; 2012. Available from: https://www.researchgate.net/publication/283498836{_}Near{_}Field{_}Communication{_}NFC{_}-{_}A{_}technical{_}Overview.

[43] Ganeshji Marwaha - Secure Element in Apple Pay; 2015. [Accessed on: 2017-10-24]. Available from: http://www.gmarwaha.com/blog/.

[44] NControl: O que é a biometria ?;. [Accessed on: 2017-10-24]. Available from: http://www.ncontrol.com.pt/o-que-e-a-biometria.html.

[45] Wilson TVH. How Biometrics Works; 2005. [Accessed on: 2017-10-24]. Available from: https://science.howstuffworks.com/biometrics.htm.

[46] Galaxy Control Systems: Access Control (Hand Geometry Reader);. [Accessed on: 2017-10-24]. Available from: http://www.galaxysys.com/category-Biometric?id=119.

[47] Keri Systems: BioPointe Fingerprint Reader;. [Accessed on: 2017-10-24]. Available from: https://www.kerisys.com/pages/products/biopointe/.

[48] Cox JTI. Iris scanners and iPhone facial recognition; 2017. [Accessed on: 2017-10-24]. Available from: http://www.independent.co.uk/voices/bitcoin-iris-scanners-facial-recognition-iphone-apple-technology-latest-reason-be-terrified-a7855466.html.

[49] Pinterest: Olho Humano;. [Accessed on: 2017-10-24]. Available from: https://www.pinterest.pt/explore/human-eye-diagram/.

[50] Pearson: Security;. [Accessed on: 2017-10-24]. Available from: http://www.pearsonpte.jp/institutions/security/.

[51] Granding Technology: Facial Recognition;. [Accessed on: 2017-10-24]. Available from: http://grandingchina.en.made-in-china.com/custom-detail/xmQExQndGJUQxmQExQndGJUQ/new-arrival-facial-recognition-with-Proximity-card-reader.html.

[52] Indiatimes: Decoding Apple iPhone X's FaceID & How Face Recognition Tech Will Soon Make Passwords Extinct;. [Accessed on: 2017-10-24]. Available from: https://www.indiatimes.com/technology/how-to/decoding-apple-iphone-x-s-faceid-how-face-recognition-tech-will-soon-make-passwords-extinct-329985.html.

[53] Carmo J. José Manuel Oliveira Carmo Sistema de Gestão e Controlo de Acessos no Setor Hoteleiro [Dissertação de Mestrado]. Universidade de Aveiro; 2014. Available from: http://hdl.handle.net/10773/13832.

[54] Sistema de controlo de acessos integrado e online; 2007. Available from: http://servicosonline.inpi.pt/pesquisas/GetSintesePDF?nord=2196931.

[55] Sistema de controlo de acessos integrado online; 2009. Available from: http://servicosonline.inpi.pt/pesquisas/GetSintesePDF?nord=3215688.

[56] Chaves do Areeiro: Kaba Oracode;. [Accessed on: 2017-10-24]. Available from: http://www.chavesareeiro.pt/Produtos/SistemasElectr{ó}nicosedeControlodeAcessos/Solu{ç}{~{o}}esparaHotelaria/KabaOracode.aspx.

[57] Chaves do Areeiro: Kaba Modelo E-790;. [Accessed on: 2017-10-24]. Available from: http://www.chavesareeiro.pt/Produtos/SistemasElectr{ó}nicosedeControlodeAcessos/Solu{ç}{~{o}}esparaHotelaria/KabaModeloE-790.aspx.

[58] 3D Plans: Modelo 3D de uma Casa;. [Accessed on: 2017-10-25]. Available from: http://3dplans.com/.

[59] Edraw: Flow Chart Design - How to design a good flowchart;. [Accessed on: 2017-11-15]. Available from: https://www.edrawsoft.com/flow-chart-design.php.

[60] Pinto PP. Endereços Públicos e Privados; 2009. [Accessed on: 2017-10-25]. Available from: https://pplware.sapo.pt/truques-dicas/enderecos-publicos-e-privados/.

[61] PayPal: Payment Data Tranfer;. Available from: https://developer.paypal.com/docs/classic/paypal-payments-standard/integration-guide/paymentdatatransfer/.

[62] TurboSMTP: What is an SMTP server;. [Accessed on: 2017-10-25]. Available from: http://www.serversmtp.com/en/what-is-smtp-server.

[63] SOS electronic: SIM900;. [Accessed on: 2017-10-25]. Available from: https://www.soselectronic.com/products/simcom/sim900-81028.

[64] Epalsite Wiki: SIM900 Quad-Band GPRS shield with Micro SD card slot;. [Accessed on: 2017-10-25]. Available from: http://wiki.epalsite.com/index.php?title=SIM900{_}Quad-Band{_}GPRS{_}shield{_}with{_}Micro{_}SD{_}card{_}slot.

[65] Microchip: PIC16F877A;. [Accessed on: 2017-10-25]. Available from: http://www.microchip.com/wwwproducts/en/PIC16F877A.

[66] Santos JP. Apontamentos Modem SIM900. Universidade de Aveiro; 2015.

[67] Microchip: SIM900 AT Command Manual; 2010. Available from: https://www.espruino.com/datasheets/SIM900{_}AT.pdf.

[68] ESP8266 learning: NodeMCU board and Arduino development; 2016. [Accessed on: 2017-10-25]. Available from: http://www.esp8266learning.com/nodemcu-board-and-arduino-development.php.

[69] The Internet of Things with ESP8266;. [Accessed on: 2017-10-25]. Available from: http://esp8266.net/.

[70] HPE: Modulo Wifi ESP8266 - 12;. [Accessed on: 2017-10-25]. Available from: http://www.hperobotica.com.br/pd-462089-modulo-wifi-esp8266-12.html.

[71] GitHub: ESP8266 DevKit;. Available from: https://github.com/nodemcu/nodemcu-devkit.

[72] Robert Oostenveld's blog: ESP-12 bootloader modes and GPIO state at startup; 2016. [Accessed on: 2017-10-25]. Available from: http://robertoostenveld.nl/esp-12-bootloader-modes/.

[73] Martyn Currey: ESP8266 and the Arduino IDE; 2017. [Accessed on: 2017-10-25]. Available from: http://www.martyncurrey.com/esp8266-and-the-arduino-ide/{#}more-5137.

[74] Alibaba: Relé Opto-Isolado;. [Accessed on: 2017-10-25]. Available from: https://portuguese.alibaba.com/product-detail/1-channel-relay-module-5v-12v-24v-with-opto-isolated-60488844012.html.

[75] Aliexpress: Sensor Magnético para porta/janela;. [Accessed on: 2017-10-25]. Available from: https://pt.aliexpress.com/store/product/20pcs-lot-Wired-Door-Window-Magnetic-Sensor-Switch-Work-With-PTSN-and-GSM-Alarm-System-Free/115772{_}711555492.html.

[76] Parallax: 4x4 Matrix Membrane Keypad; 2011. [Accessed on: 2017-10-25]. Available from: https://www.parallax.com/sites/default/files/downloads/27899-4x4-Matrix-Membrane-Keypad-v1.2.pdf.

[77] GRAFCET (Norma IEC 848);. Available from: http://ftp.demec.ufpr.br/disciplinas/TM265/GRAFCET{_}utfpr{_}iec{_}848.pdf.

[78] Random Nerd Tutorials: ESP8266 ADC;. Available from: http://randomnerdtutorials.com/esp8266-adc-reading-analog-values-with-nodemcu/.

Apêndices

Apêndice A

Páginas da Plataforma de Reservas

Este apêndice procura apresentar alguns *prints* das páginas desenvolvidas para a plataforma de reservas. A sequência seguida na apresentação das imagens assemelha-se, de certo modo, à sequência de páginas apresentadas durante o processo de reserva. As páginas de *Login* do Utilizador e de Monitorização da Informação relativa ao Administrador dos espaços e ao Cliente não obedecem à sequência de páginas do processo de reservas, sendo consideradas páginas isoladas.

As páginas apresentadas nas imagens seguintes são (por ordem):

- Página Inicial (Figuras A.1, A.2, A.3 e A.4);
- Página de Requisitos da Reserva (Figuras A.5 e A.6);
- Página - Carrinho de Compras (Figuras A.7 e A.8);
- Página de Confirmação de dados e Pagamento (Figuras A.9 e A.10);
- "PayPal" (Figura A.11);
- Página de Sucesso/Insucesso (Figuras A.12 e A.13);
- Página de *Login* do Utilizador (Figuras A.14, A.15 e A.16);
- Página de Monitorização do Cliente e do Administrador (Figuras A.17, A.18, A.19, A.20, A.21, A.22, A.23, A.24, A.25 e A.26).

Figura A.1: Página Inicial - 1.

Figura A.2: Página Inicial - 2.

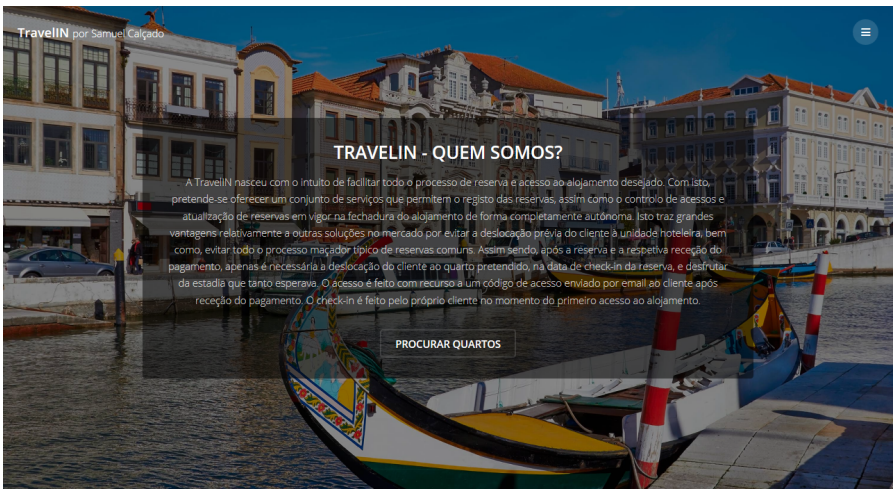


Figura A.3: Página Inicial - 3.

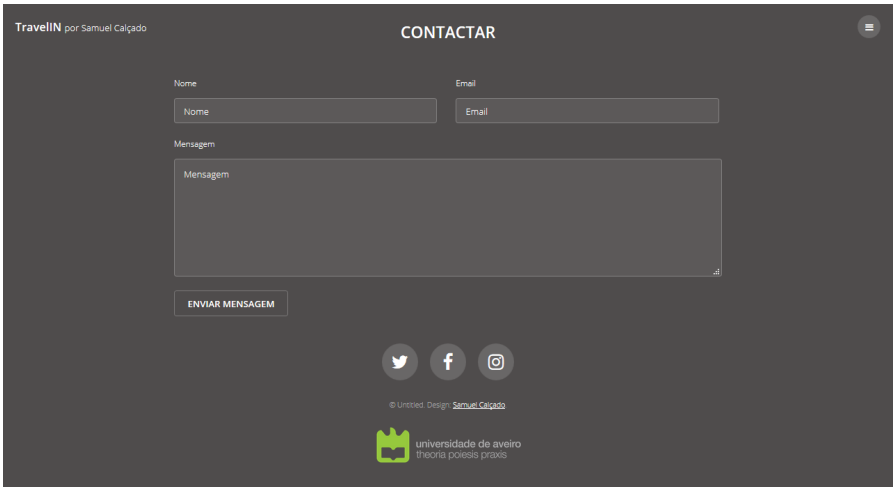


Figura A.4: Página Inicial - 4.

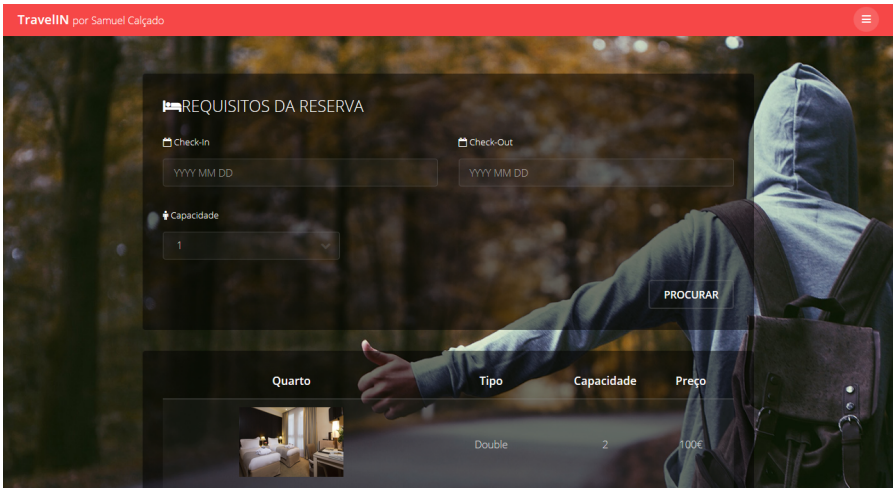


Figura A.5: Página de Requisitos da Reserva - 1.

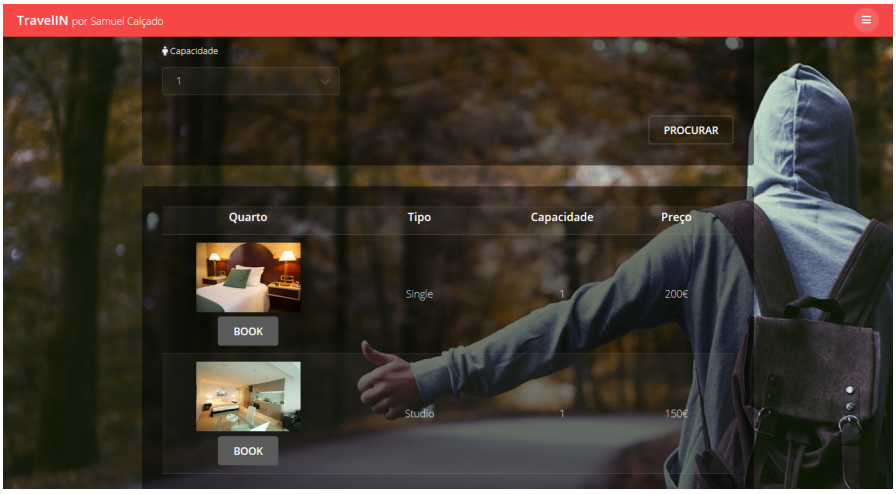


Figura A.6: Página de Requisitos da Reserva - 2.

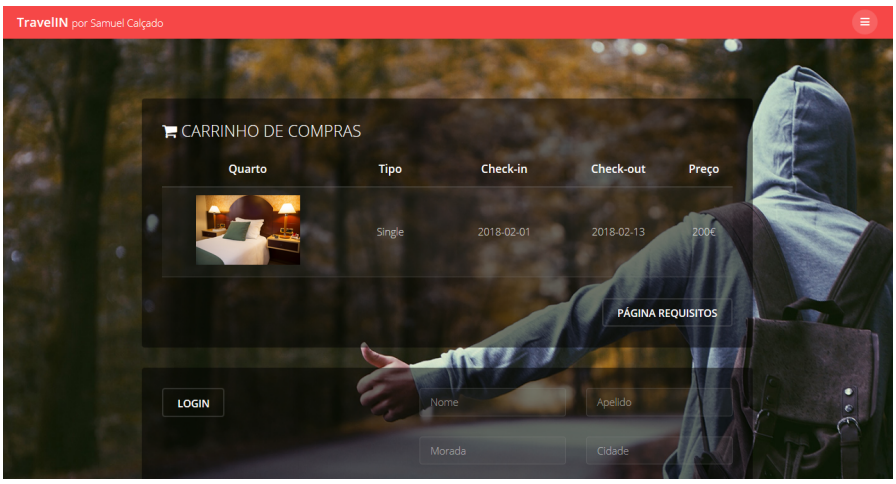


Figura A.7: Página de Carrinho de Compras - 1.

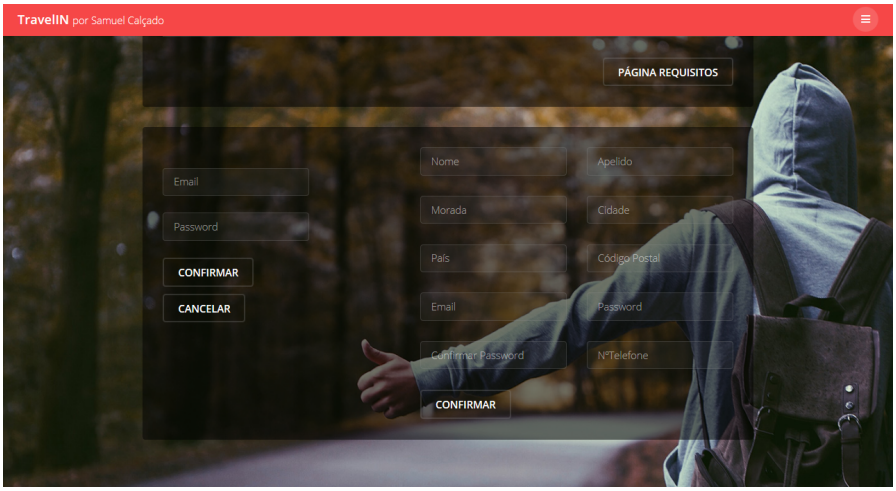


Figura A.8: Página de Carrinho de Compras - 2.

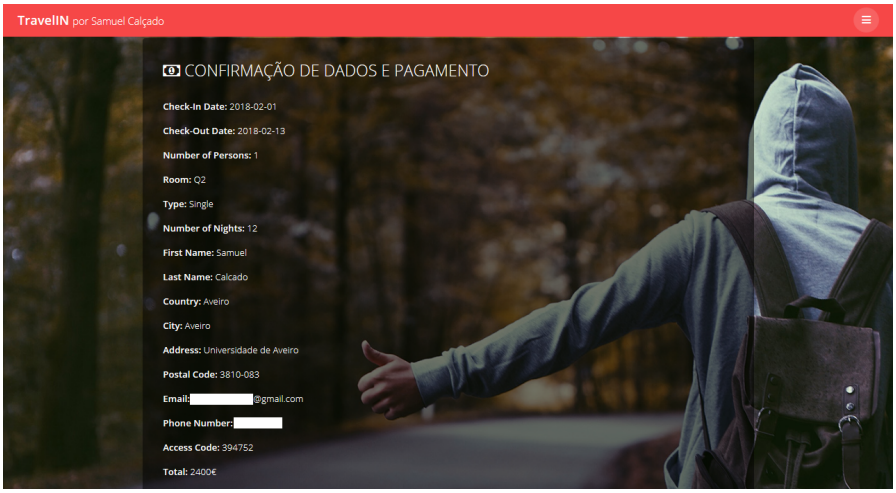


Figura A.9: Página de Confirmação de Dados e Pagamento - 1.

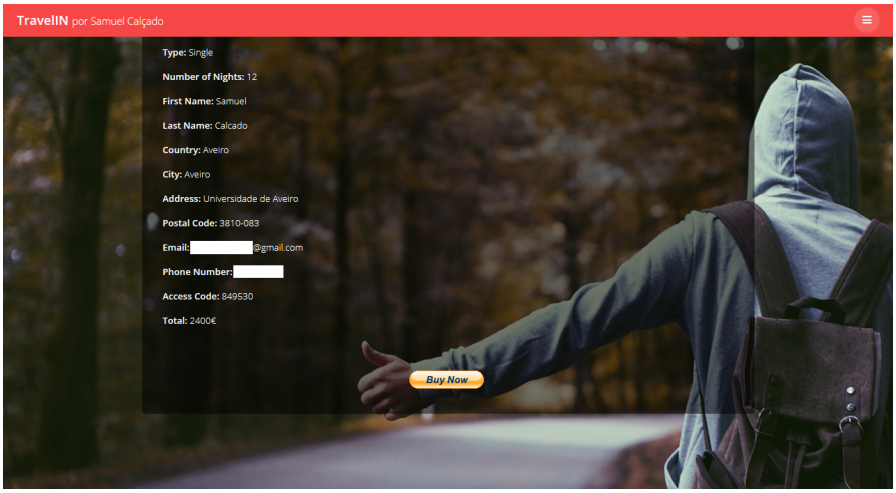


Figura A.10: Página de Confirmação de Dados e Pagamento - 2.

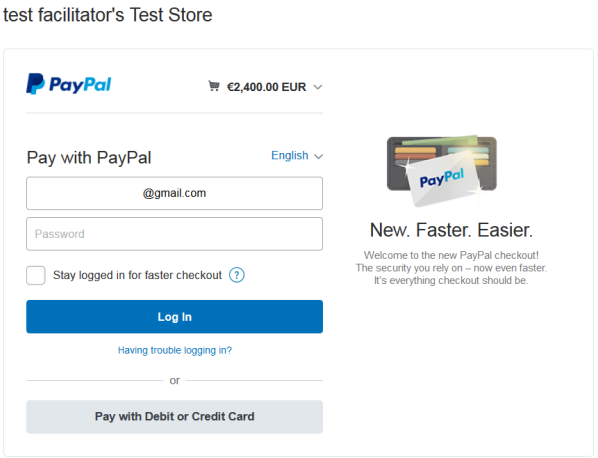


Figura A.11: "PayPal" - 1.

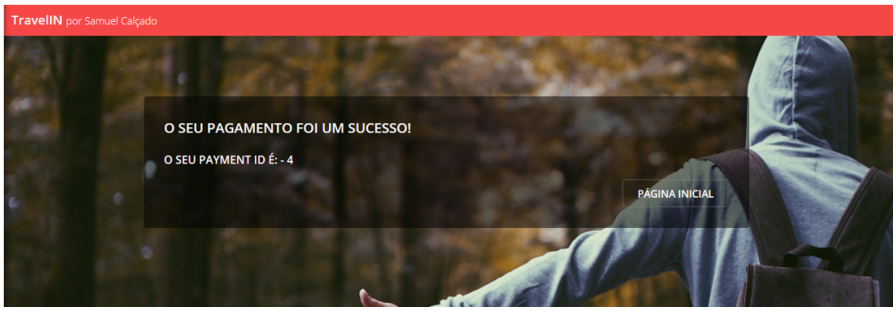


Figura A.12: Página de Sucesso - 1.

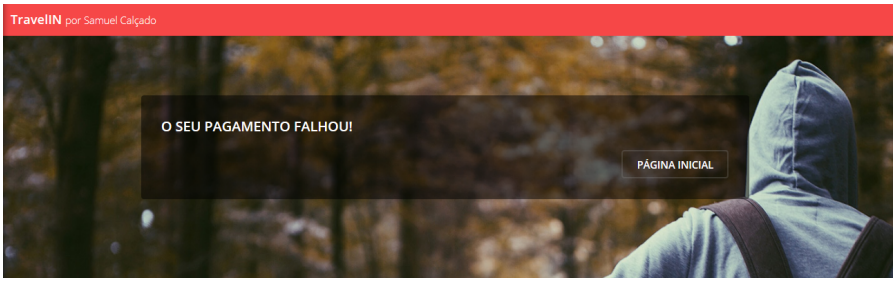


Figura A.13: Página de Insucesso - 1.

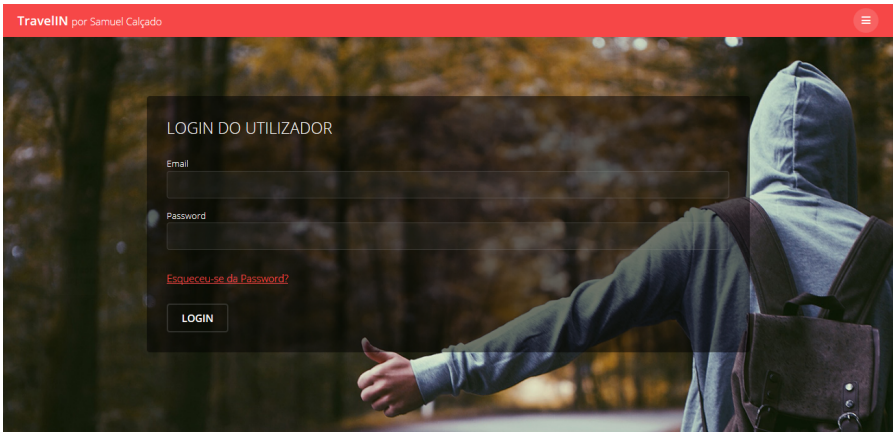


Figura A.14: Página de *Login* do Utilizador - 1.

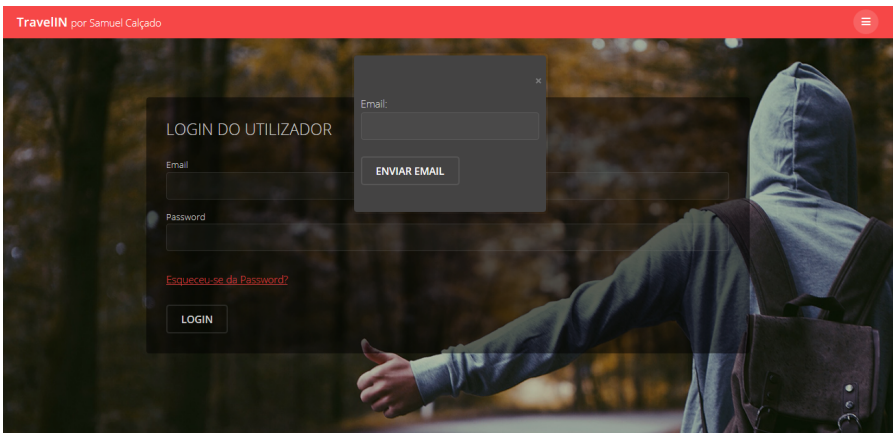


Figura A.15: Página de *Login* do Utilizador - 2.

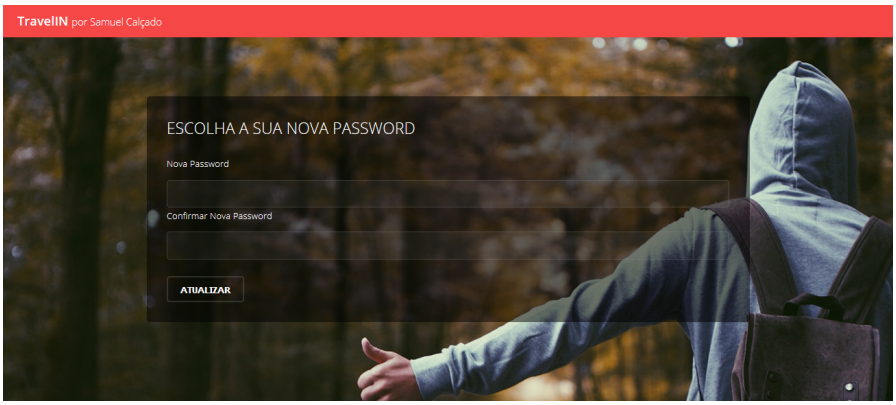


Figura A.16: Página de *Login* do Utilizador - 3.

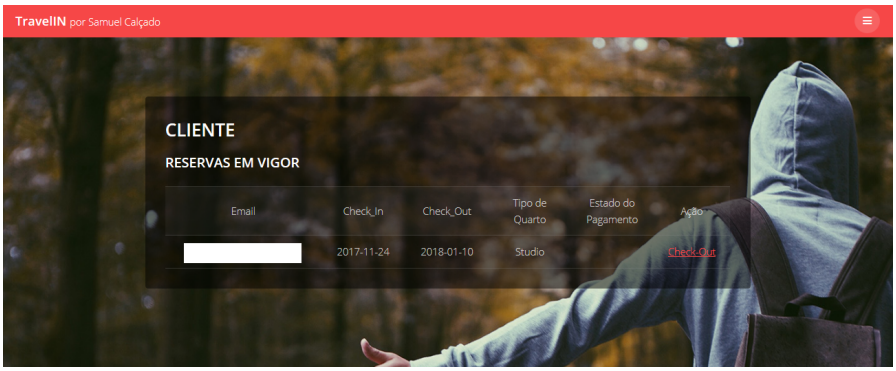


Figura A.17: Página de Monitorização do Cliente - 1.

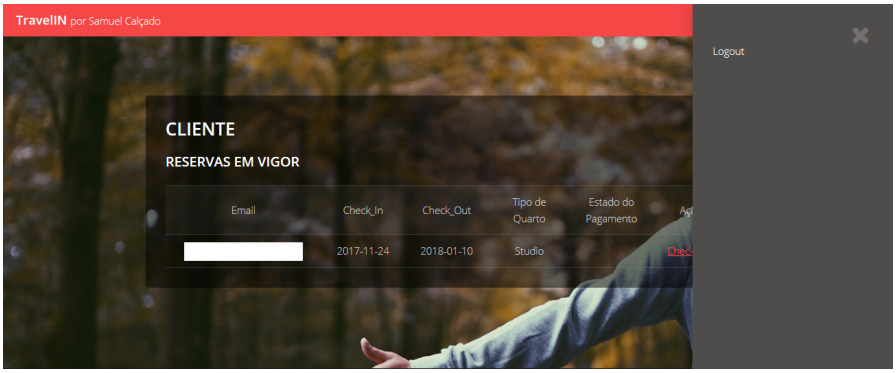


Figura A.18: Página de Monitorização do Cliente - 2.

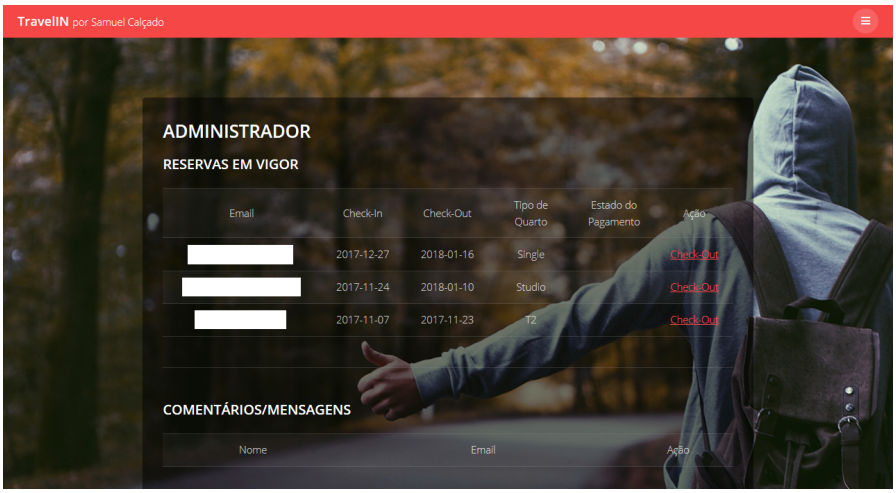


Figura A.19: Página de Monitorização do Administrador - 1.

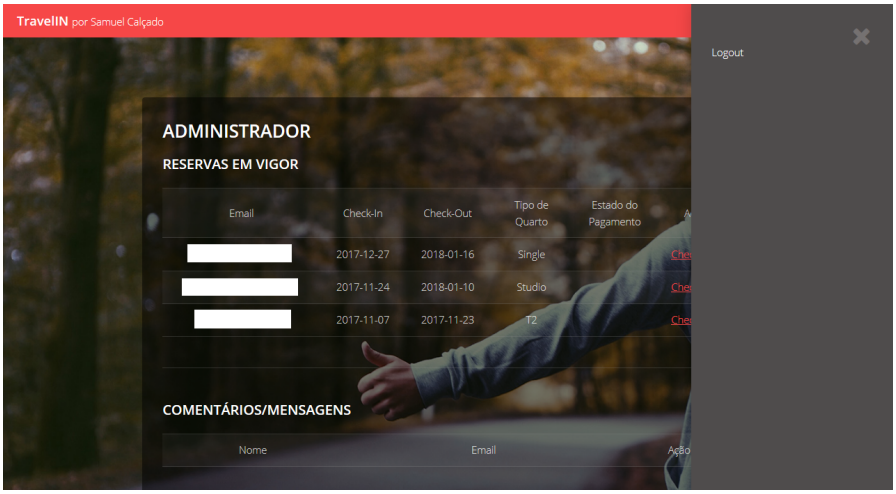


Figura A.20: Página de Monitorização do Administrador - 2.

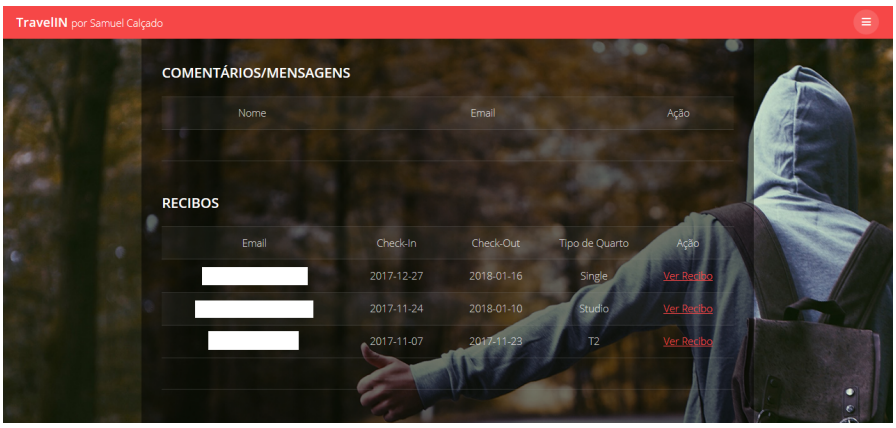


Figura A.21: Página de Monitorização do Administrador - 3.

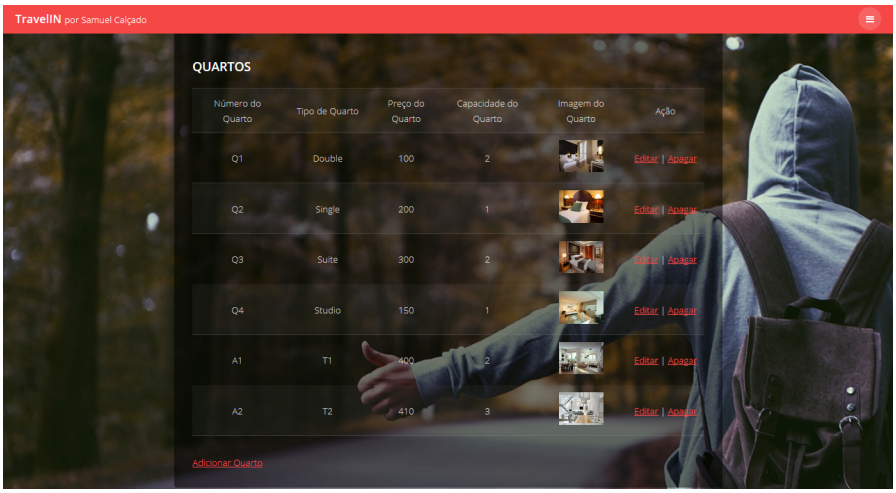


Figura A.22: Página de Monitorização do Administrador - 4.

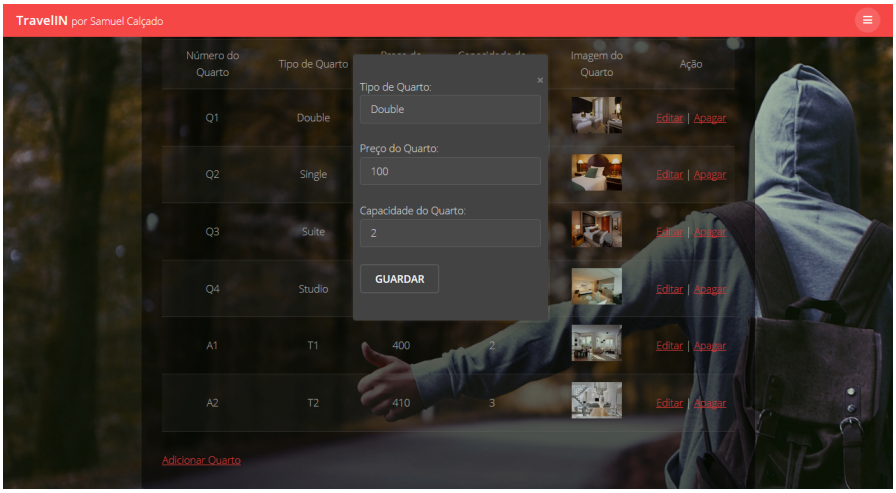


Figura A.23: Página de Monitorização do Administrador - 5.

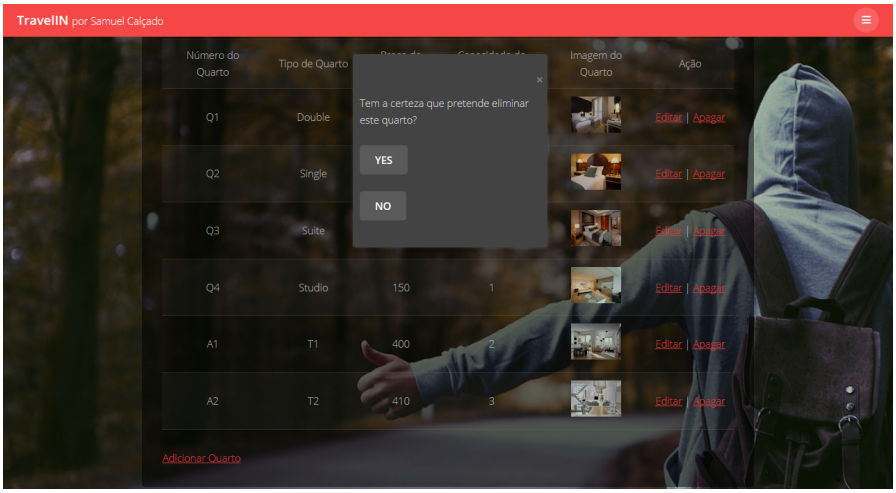


Figura A.24: Página de Monitorização do Administrador - 6.

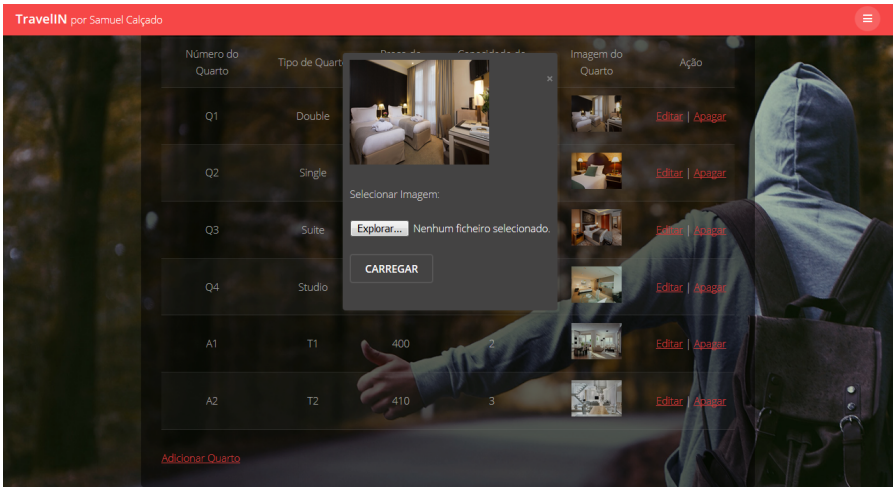


Figura A.25: Página de Monitorização do Administrador - 7.

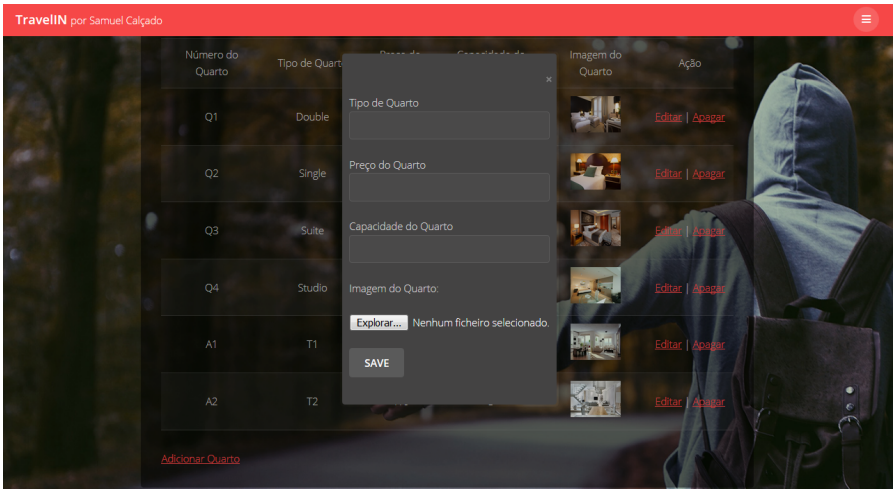


Figura A.26: Página de Monitorização do Administrador - 8.

Apêndice B

Configuração do servidor de *emails* "Mercury"

A comunicação com o cliente para envio da informação pertinente relativa à sua reserva leva à necessidade de utilização de um servidor dedicado de *emails*.

Nesta situação, com vista no aproveitamento do *software* já instalado, foi utilizada uma ferramenta do XAMPP denominada "Mercury". Esta ferramenta consiste num servidor de *emails* que permite o envio de mensagens aos clientes de forma automática, após respetiva reserva.

Para o envio de *emails* através de páginas PHP, apenas é necessário utilizar a função "mail()" com os campos desejados constituintes da mensagem.

As imagens seguintes procuram ilustrar a configuração do "Mercury" para o envio de *emails* através do "Gmail" (protocolo SMTP).

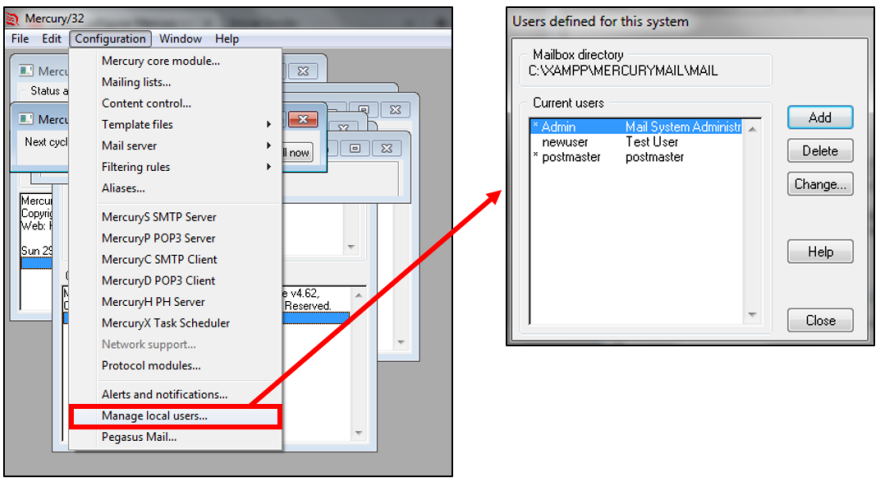


Figura B.1: 1º - *Manage Local Users*.

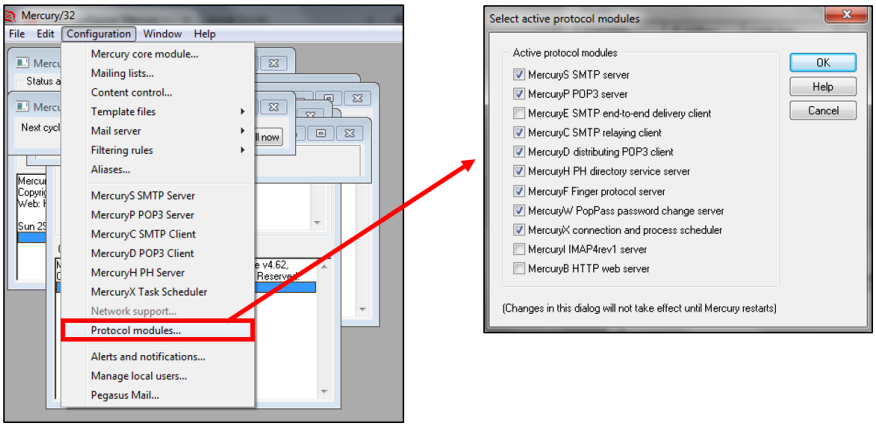


Figura B.2: 2º - *Protocol Modules*.

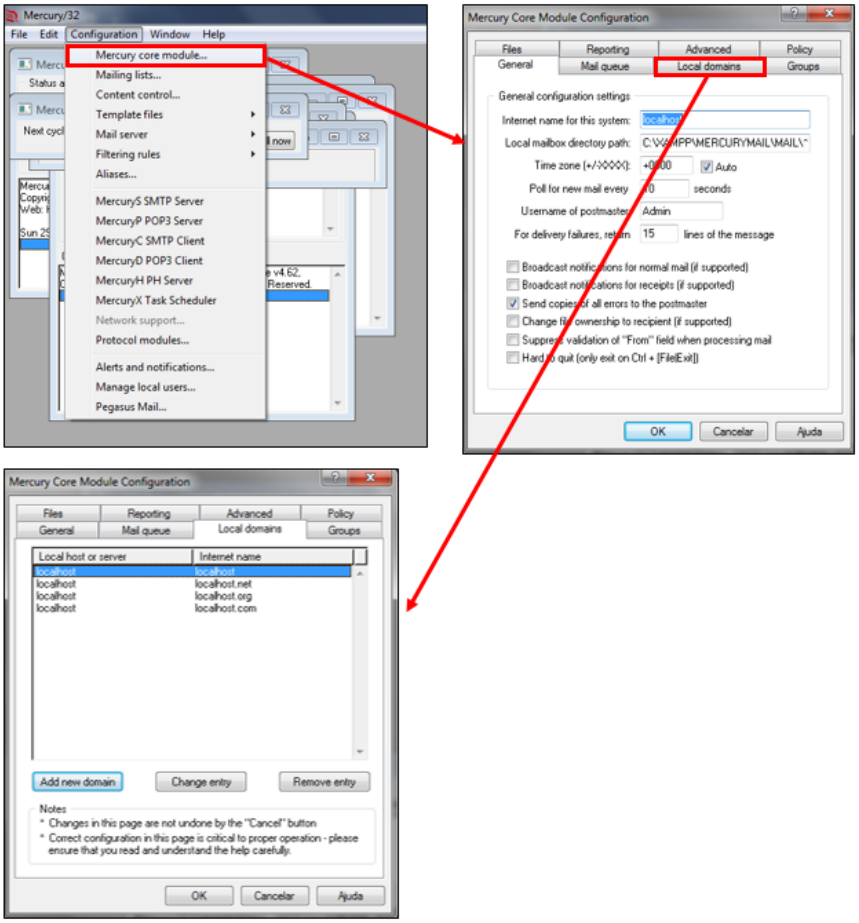


Figura B.3: 3º - "Mercury" *Core Module e Local Domain*.

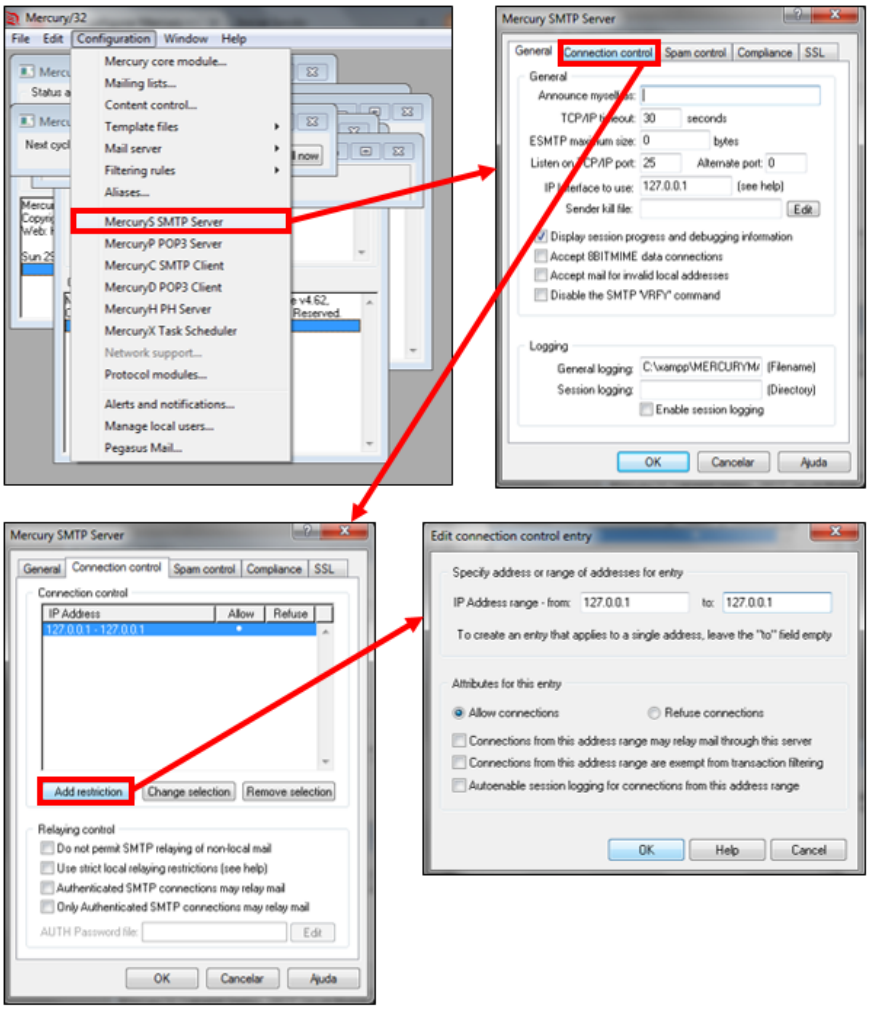


Figura B.4: 4º - Definições SMTP *Server*.

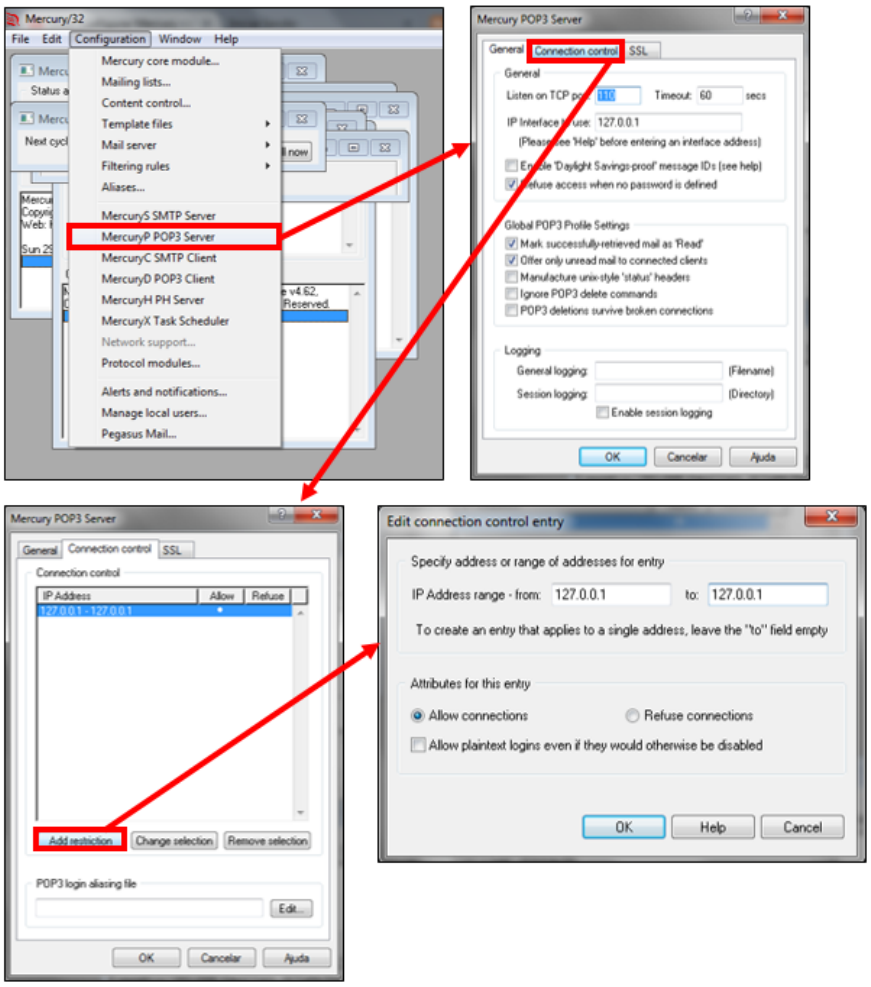


Figura B.5: 5º - Definições POP3 *Server*.

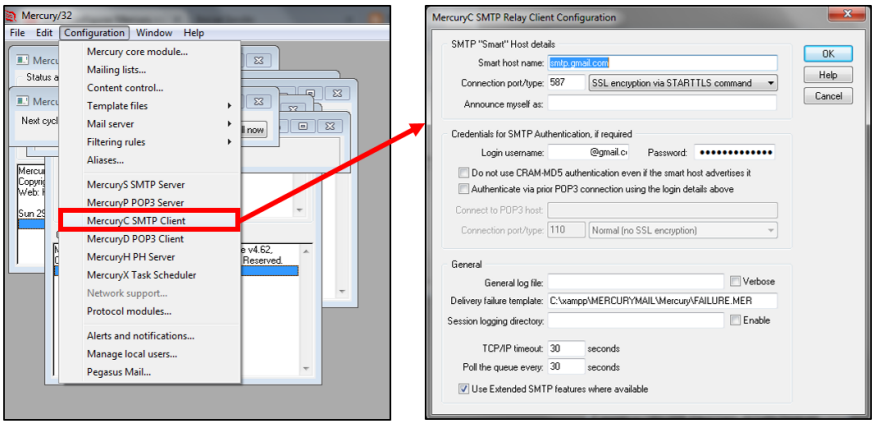


Figura B.6: 6º - Definições SMTP *Client*.

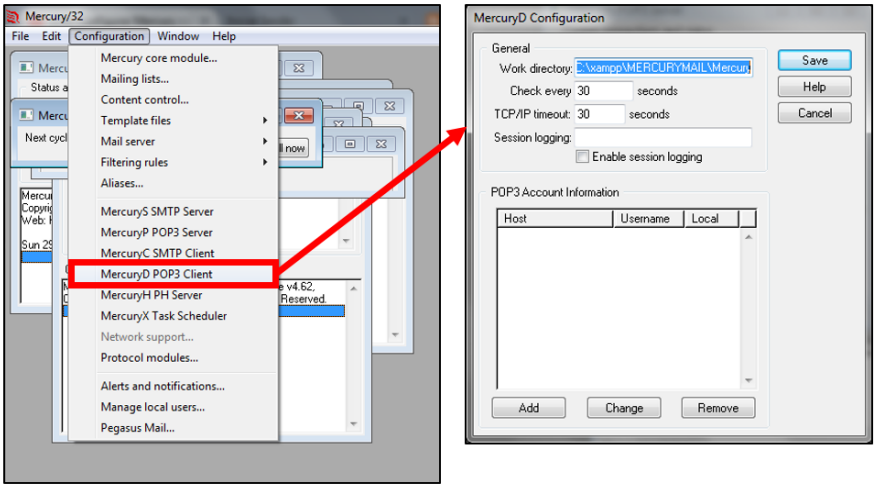


Figura B.7: 7º - Definições POP3 *Client*.

Após as configurações expostas anteriormente estarem concluídas, resta apenas fazer o teste de envio de um *email* através do "Mercury". Os *emails* enviados através da aplicação são enviados por uma conta de *email* do "Gmail", definida na Figura B.6.

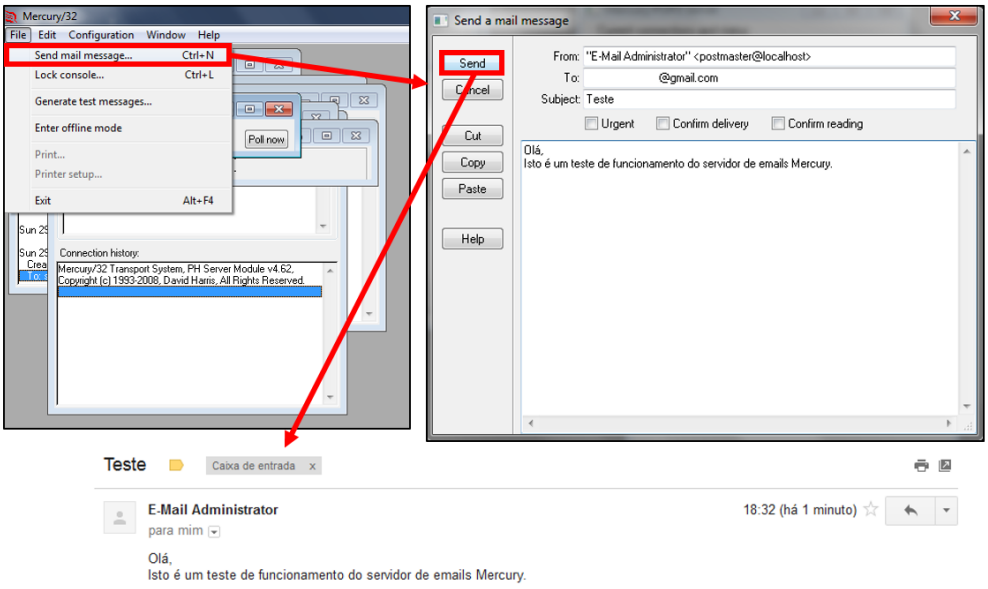


Figura B.8: 8º - Teste de envio de *email* pelo "Mercury".

Para poder enviar *emails* através de uma página PHP, é necessário configurar o ficheiro "PHP.ini" do "Apache". Esta configuração permite ao "Apache" o reencaminhamento dos *emails* pedidos nas páginas PHP para o servidor de *emails* "Mercury".

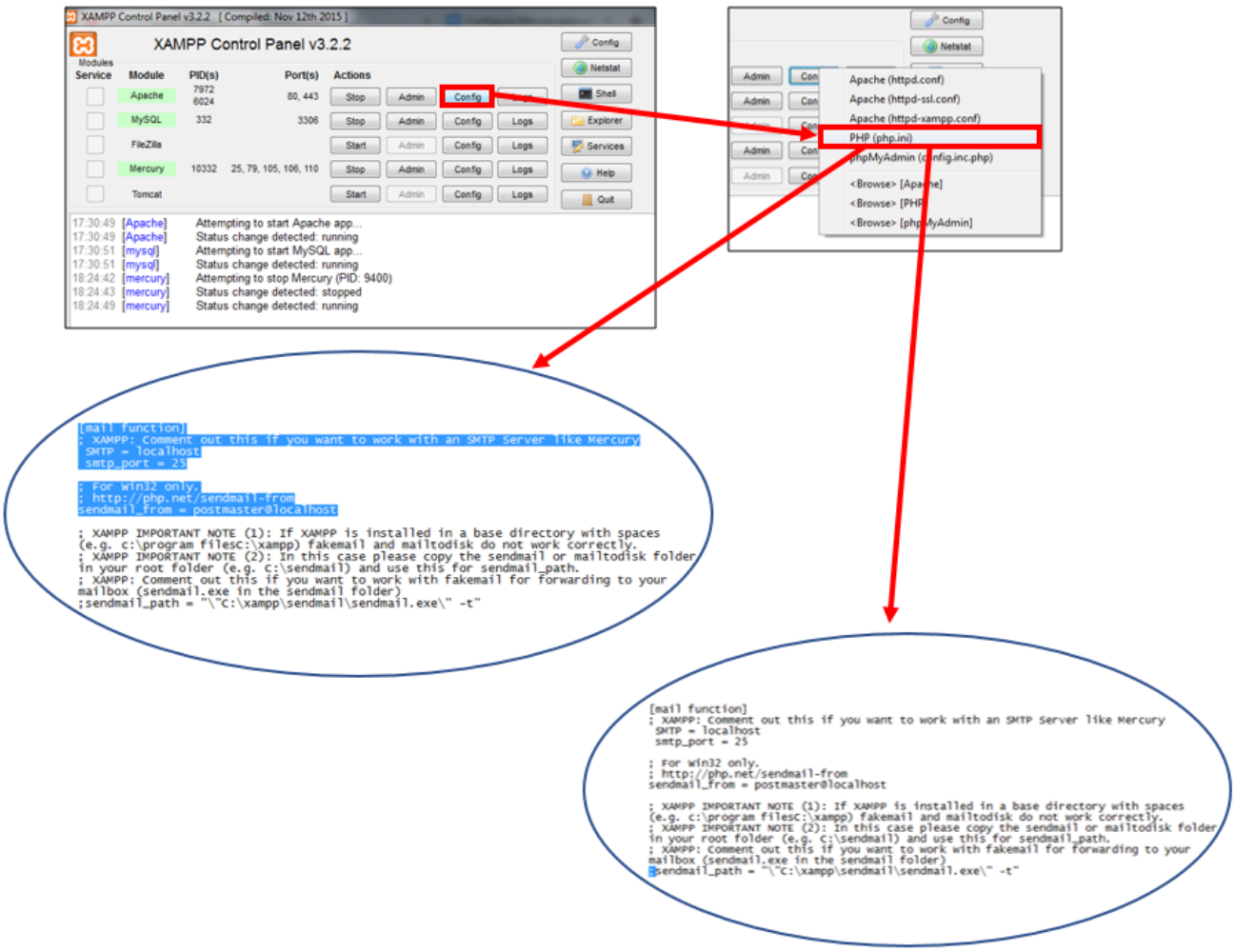


Figura B.9: 9º - Configurar ficheiro "PHP.ini".

Apêndice C

Configuração do *router* para a comunicação SIM900

Uma das soluções propostas para a comunicação entre a fechadura do alojamento, o servidor WEB "Apache" e a base de dados do sistema reside na utilização de uma *shield* GSM/GPRS SIM900.

Na ausência de um servidor dedicado com IP Público, a necessidade de simular a comunicação num ambiente doméstico levou à configuração de um *router*, para garantir a chegada de pedidos HTTP a um computador da sua rede local.

Essa configuração permite a passagem de pedidos de ligação TCP pela porta 80, entre o SIM900 e o computador local com o XAMPP instalado (para simular o servidor WEB e de base de dados).

As Figuras C.1 e C.2, ilustram essa configuração aplicada num *router* "Technicolor TG784n v3".

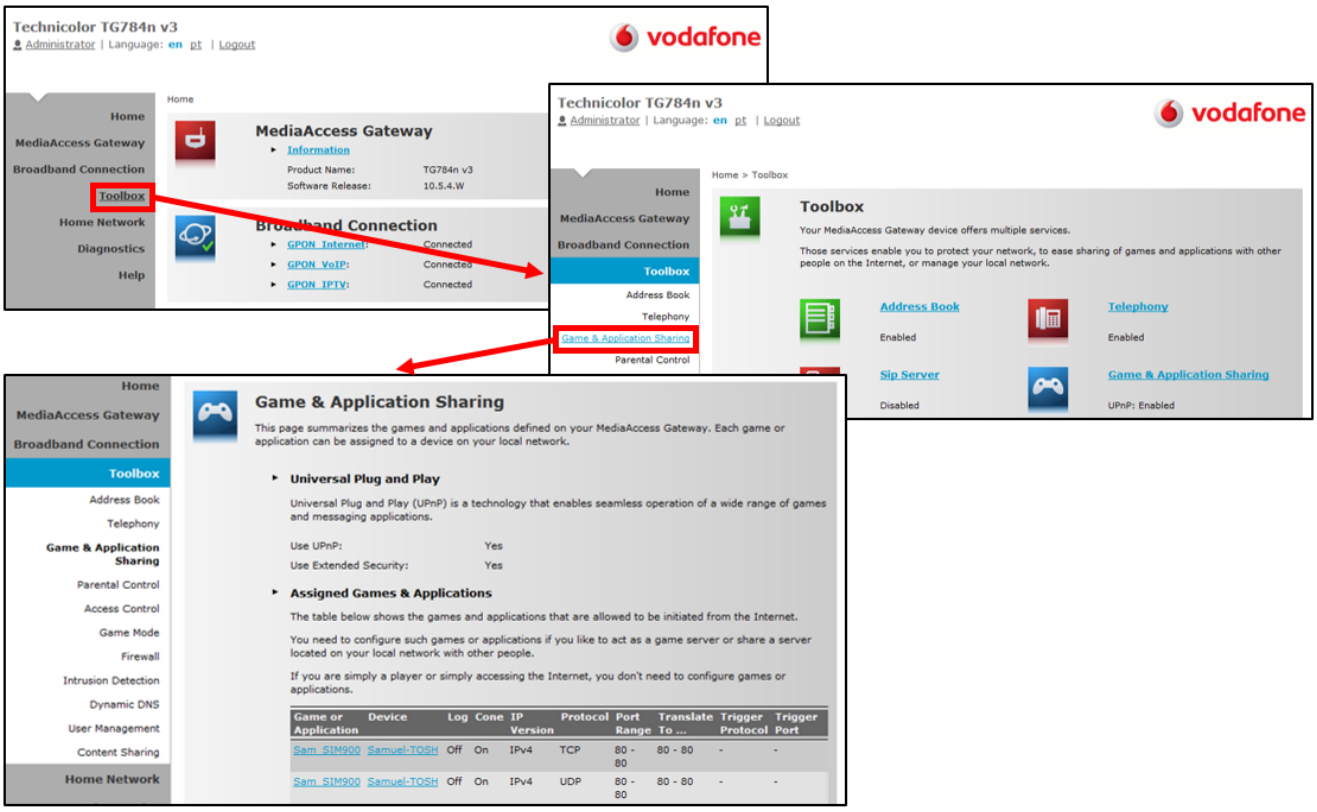


Figura C.1: Página de *Game & Application Sharing*.

Na página de *Game & Application Sharing* é necessário criar uma nova restrição que permita dar autorização ao *router* para deixar passar as ligações TCP destinadas a determinada porta (neste caso, à porta 80).

Após a criação dessa restrição, é necessário reencaminhar os pedidos de ligação recebidos para um dispositivo da rede conectado ao *router*. (Ver Figura C.2)

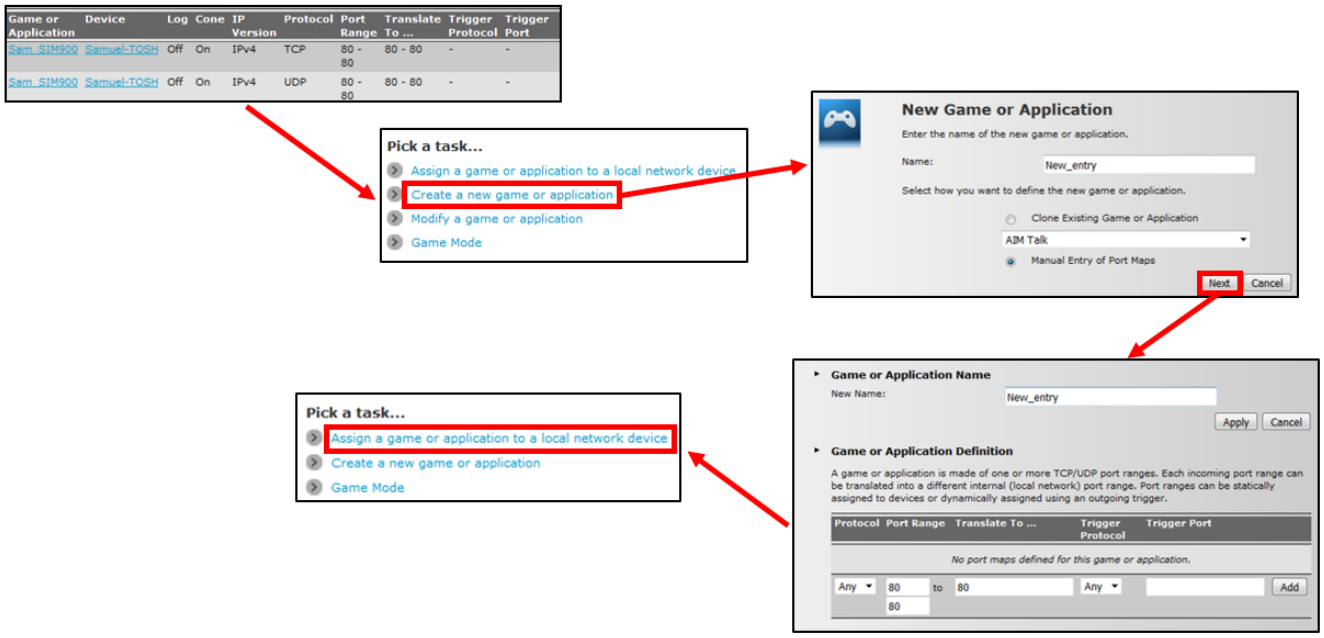


Figura C.2: Criar nova restrição e relacioná-la com dispositivo conectado ao *router*.

Apêndice D

Comandos AT utilizados no programa SIM900

Os Comandos AT utilizados no programa SIM900 para comunicação com a base de dados do sistema estão representados na Tabela D.1.

Tabela D.1: Comandos AT para ligação TCP.

Comando AT	**Descrição**	**Resposta**
AT	Este comando é utilizado para verificar se existe conexão entre os dois equipamentos.	OK / ERROR
ATE0	Não mostra os comandos AT enviados para o *modem*.	OK / ERROR
AT+CPIN=0523	Permite introduzir o PIN no cartão SIM.	OK / ERROR / +CME ERROR
AT+CGATT=1	Liga *modem* ao serviço GPRS.	OK / ERROR / +CME ERROR
AT+CIPMUX=0	Permite configurar o *modem* para ter apenas uma porta aberta para conexões externas.	OK / ERROR
AT+CSTT="internet", "guest", "guest"	Permite conectar o *modem* à Internet. Os parâmetros utilizados são ("APN", "USERNAME", "PASSWORD"), neste exemplo configurados para a MEO.	OK / ERROR
AT+CIICR	Assegura ligação da rede sem fios. Verifica se o *modem* tem um SIM com crédito para efetuar a ligação de dados.	OK / ERROR
AT+CIFSR	Retorna o IP atribuído pela rede móvel ao *modem*.	<IP> / ERROR

AT+CIPSTART=“TCP”, “193.137.172.20”, “80”	Estabelece uma ligação TCP entre o *modem* e um computador remoto com o IP “193.137.172.20” na sua porta 80.	OK / +CME ERROR
AT+CIPSEND=31	Permite enviar uma mensagem de texto para o servidor. Neste caso, após o *modem* responder com a autorização de envio da mensagem (>), é feito um pedido de uma página PHP que atualiza e lê informação da Base de Dados (GET /teste_ tese.php?).	SEND OK / +CME ERROR / SEND FAIL
AT+CIPCLOSE	Termina a ligação TCP.	CLOSE OK / ERROR
AT+CIPSHUT	Fecha a porta de comunicação TCP.	SHUT OK / ERROR
AT+CGATT=0	Desliga *modem* do serviço GPRS.	OK / ERROR / +CME ERROR

Apêndice E

"Grafcet" da comunicação SIM900

Para o controlo dos processos sequenciais inerentes ao desenvolvimento de um programa, é normalmente utilizada uma metodologia denominada "Grafcet" (*Graphe Fonctionnel de Commande, Étapes Transitions*).

Na Figura E.1 é apresentado o "Grafcet" do programa desenvolvido para envio de comandos AT para o SIM900 e posterior interpretação da resposta do servidor WEB ao pedido HTTP feito pelo módulo [77].

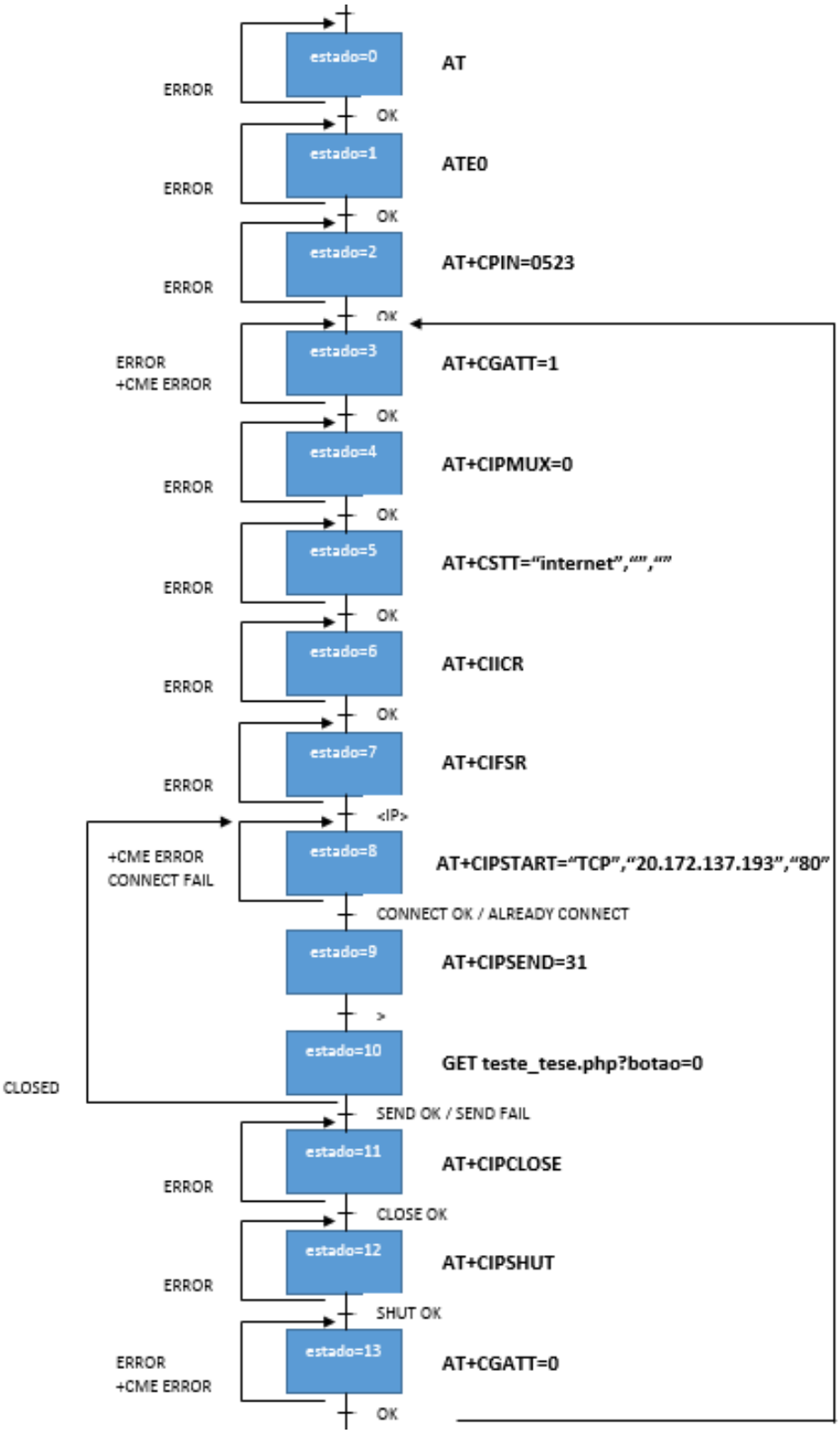


Figura E.1: “Grafcet” da comunicação SIM900 - Servidor WEB.

Apêndice F

Esquema do módulo para a comunicação entre SIM900 e o servidor

A Figura F.1 representa o esquema desenvolvido para a simulação da comunicação entre o módulo SIM900 e o servidor WEB (O servidor WEB é quem faz os pedidos SQL ao servidor Base de Dados).

Este esquema contém um microcontrolador PIC16F877, para controlo do envio de comandos AT para o SIM900, envio de pedidos HTTP para o servidor WEB e interpretação das mensagens de resposta aos pedidos efetuados.

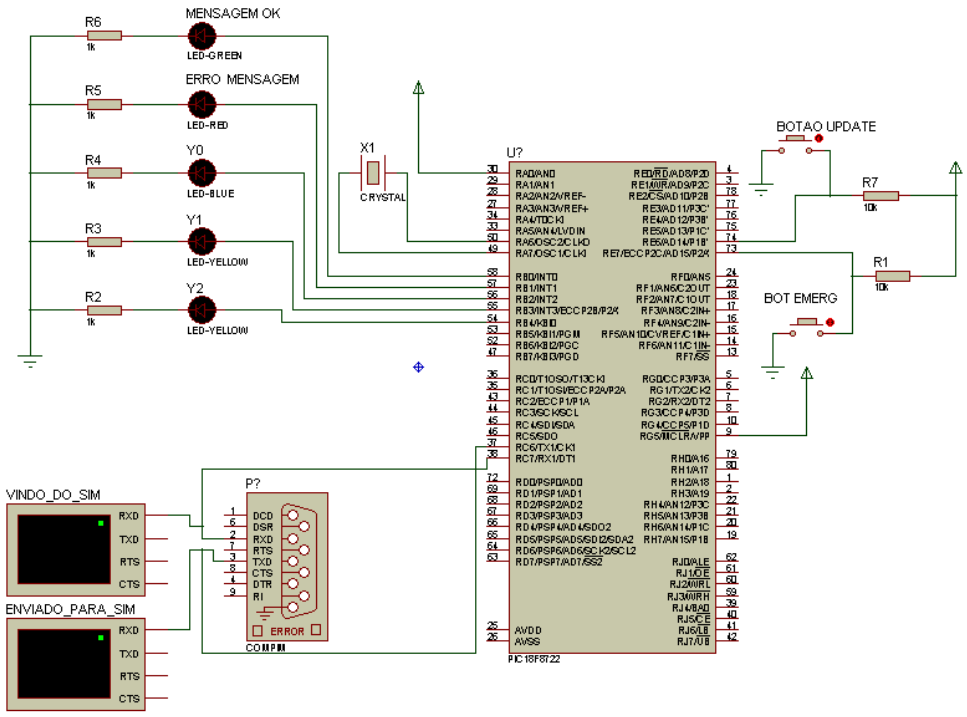


Figura F.1: Esquema do circuito desenvolvido para a comunicação SIM900.

Apêndice G

Divisor resistivo para leitura do Teclado

Na solução proposta, a leitura e interpretação das teclas pressionadas foi conseguida com auxílio da placa de desenvolvimento NodeMCU. Na ligação do Teclado à placa surge um problema relativo ao número de pinos necessários para a conexão entre os dois equipamentos.

Uma solução viável para este problema passa pela utilização do pino analógico da placa e, posteriormente, do divisor resistivo.

O divisor resistivo existe com o intuito de gerar uma tensão diferente para cada tecla pressionada, sendo que a entrada analógica e respetivo conversor ADC de 10 bits permitem a conversão da tensão gerada em valores ADC de 0 a 1024 (0-0V e 1024-12V).

Esses valores são posteriormente utilizados no programa desenvolvido, para controlo de acessos ao alojamento, para a identificação das teclas pressionadas.

A matriz seguinte (Figura G.1) procura representar a disposição das teclas do teclado utilizado no desenvolvimento desta solução. A identificação das linhas e das colunas apenas serve de guia para o cálculo das tensões resultantes do pressionar de teclas.

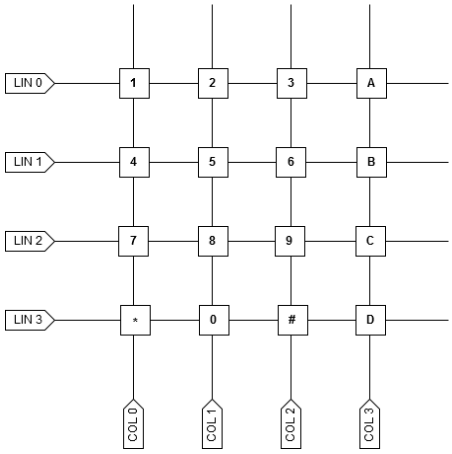


Figura G.1: Matriz do Teclado.

Para diferenciar os valores de tensão resultantes do pressionar de teclas, é utilizado um pequeno divisor resistivo, no qual cada tecla assume uma combinação linha-coluna da matriz do teclado (Ver Tabela G.1).

Tabela G.1: Disposição das Teclas na Matriz do Teclado.

Teclas	**1**	**2**	**3**	**A**	**4**	**5**	**6**	**B**	**7**	**8**	**9**	**C**	*	**0**	#	**D**
Linha	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3
Coluna	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3

A Figura G.2 apresenta o circuito proposto para a leitura do teclado com todos os componentes e ligações necessárias ao seu funcionamento. É importante salientar que a tensão de entrada utilizada é de 5V, sendo necessário garantir à saída (A0) uma tensão não superior a 3.3V (para não danificar o ESP, pois a ADC apenas consegue converter tensões entre os 0V e os 3.3V) [78].

A resistência R6 e o condensador C1 têm a funcionalidade de filtro do sinal recebido, para estabilização do valor de tensão lido na porta analógica (Circuito RC - Filtro Passa-Baixo).

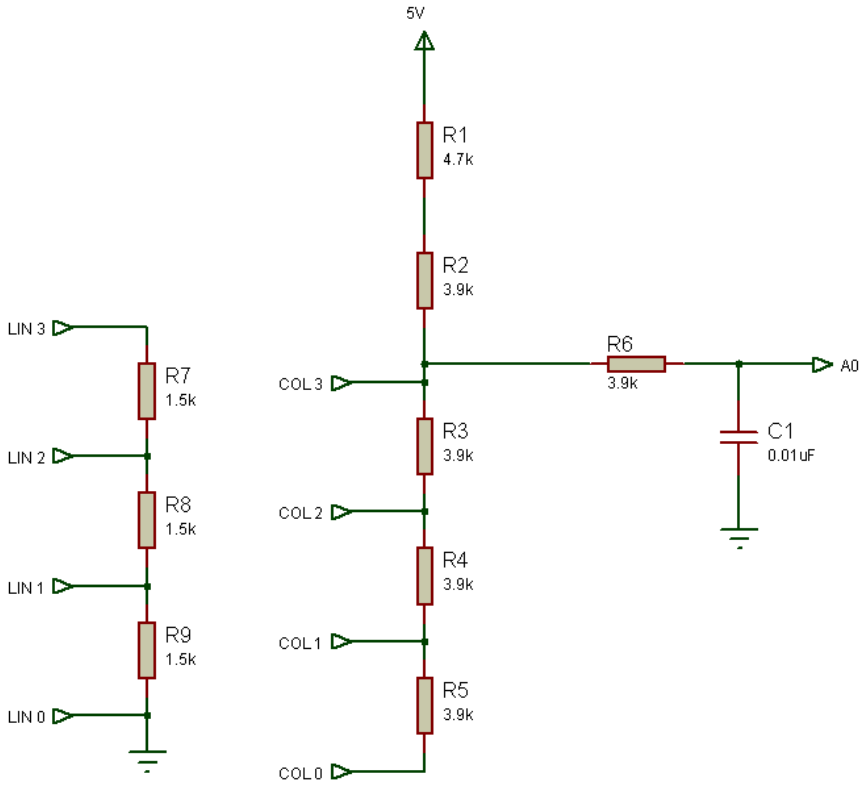


Figura G.2: Divisor Resistivo do Sistema.

O cálculo das tensões lidas na porta analógica teve em consideração a seguinte definição para obtenção da tensão resultante num divisor resistivo (Figura G.3):

$$V_{out} = \frac{R_{eq2}}{R_{eq1} + R_{eq2}} \cdot V_{in} \tag{G.1}$$

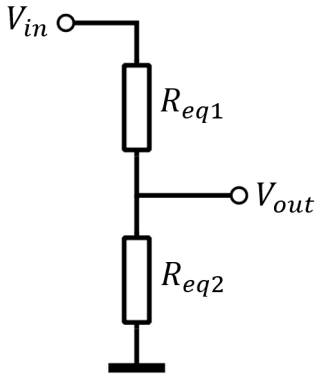


Figura G.3: Definição de Divisor Resistivo.

Comparando a Figura G.3 com a Figura G.2, é possível concluir que $R_{eq1} = R_1 + R_2$, ou seja, $R_{eq1} = 4700 + 3900 = 8600\,\Omega$. A adição de uma resistência de $3900\,\Omega$ acontece exclusivamente com o propósito de baixar a tensão de saída V_{out} para valores abaixo dos 3.3V.

A R_{eq2}, por sua vez, varia consoante a tecla premida, sendo a soma de resistências feita consoante o par linha-coluna apresento na Tabela G.1.

O teclado utilizado contém 8 pinos de ligação para interface com a restante montagem: 4 para as linhas (LIN 0, LIN 1, LIN 2 e LIN 3) e outros 4 para as colunas (COL 0, COL 1, COL 2 e COL 3).

O cálculo das resistências equivalentes teve em consideração a regra para a soma de resistências em série:

$$R_{eq} = R_1 + R_2 + R_3 + \cdots + R_n \tag{G.2}$$

A Tabela G.2 apresenta os valores de R_{eq2}, bem como os valores de tensão de saída (V_{out}) tomados com o pressionar de cada tecla.

Tabela G.2: Valores de R_{eq2} e V_{out}.

Teclas	**1**	**2**	**3**	**A**	**4**	**5**	**6**	**B**	**7**	**8**	**9**	**C**	*	**0**	#	**D**
$R_{eq2}(\Omega)$	11,7	7,8	3,9	0	13,2	9,3	5,4	1,5	14,7	10,8	6,9	3	16,2	12,3	8,4	4,5
V_{out}**(V)**	2,88	2,38	1,56	0	3,03	2,60	1,93	0,74	3,15	2,78	2,23	1,29	3,27	2,94	2,47	1,72

A ADC utilizada na conversão dos valores analógicos de tensão em valores digitais possui uma resolução de 10 bits, ou seja, com valores entre 0 e 1023 (pois $2^{10} = 1024$). A obtenção dos valores ADC pode ser feita de duas formas: através de um programa descarregado na memória do ESP, ou manualmente, através de uma pequena proporção:

$$\frac{1023}{3,3} = \frac{ValorADC}{V_{out}} \tag{G.3}$$

O valor resultante, obtido pela conversão analógico-digital de uma tensão de 3,3V, é de, aproximadamente, 1023. A Tabela G.3 ilustra os valores ADC obtidos manualmente, comparados aos valores obtidos pelo programa ESP.

Tabela G.3: Comparação de valores obtidos manualmente com valores retirados de programa para leitura da porta analógica.

Teclas	**1**	**2**	**3**	**A**	**4**	**5**	**6**	**B**	**7**	**8**	**9**	**C**	*	**0**	#	**D**
V_{out}**(V)**	2,88	2,38	1,56	0	3,03	2,60	1,93	0,74	3,15	2,78	2,23	1,29	3,27	2,94	2,47	1,72
Valor ADC obtidos manualmente	892,8	737,8	483,6	0	939,3	806	598,3	229,4	976,5	861,8	691,3	399,9	1013,7	911,4	765,7	533,2
Valor ADC obtidos por programa	882	729	480	7	930	795	591	233	967	851	684	402	1000	901	756	529

É importante referir a semelhança entre os dados obtidos manualmente e os adquiridos pelo programa ESP de leitura da porta analógica. Posto isto, resta apenas, no programa de controlo da fechadura, comparar os valores lidos pelo pressionar de teclas (no momento desejado para acesso ao alojamento) com os valores adquiridos previamente na conversão ADC (Tabela G.3).

Apêndice H

Esquemas Elétricos das placas PCB

As Figuras H.1 e H.2 procuram ilustrar as duas placas PCB desenvolvidas para a solução proposta nesta dissertação. A sub-divisão das placas, tal como referido anteriormente, acontece apenas por razões de segurança.

Dessa forma, são propostas duas placas PCB:

- Placa de Alimentação e Comunicação (Figura H.1);
- Placa de ligação do Teclado (Figura H.2).

Para evitar possíveis entradas indesejadas com o acesso ao cabo de alimentação da fechadura, a placa de alimentação é colocada no interior do alojamento. No exterior apenas fica a placa do teclado com o divisor resistivo, que permite a posterior leitura das teclas pressionadas.

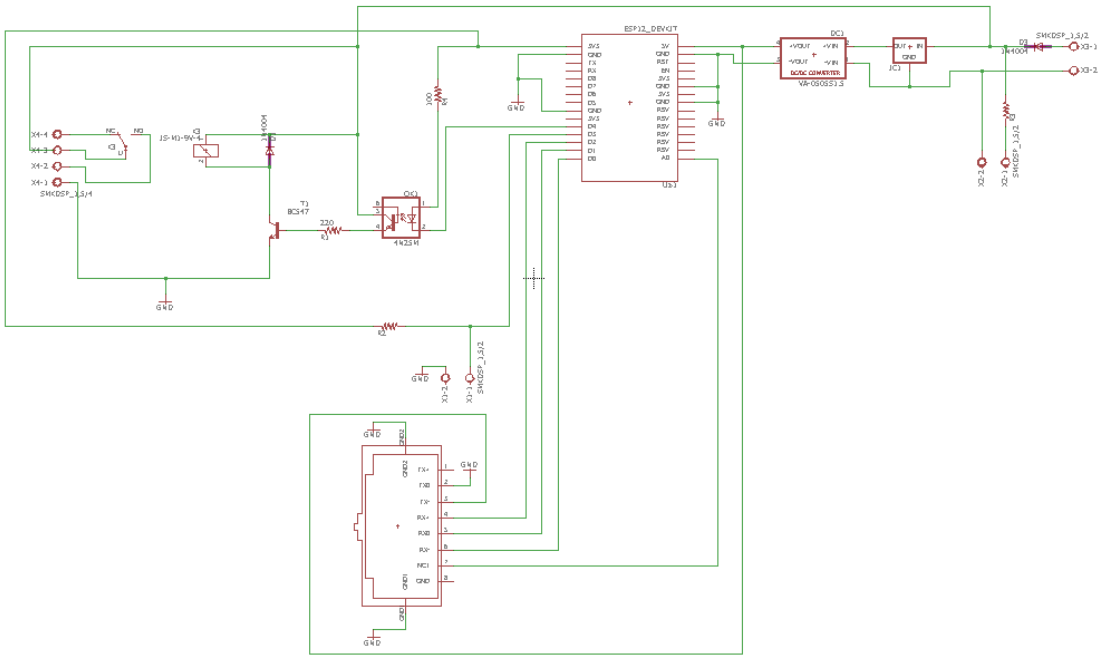


Figura H.1: Circuito Elétrico da Placa de Alimentação e Comunicação.

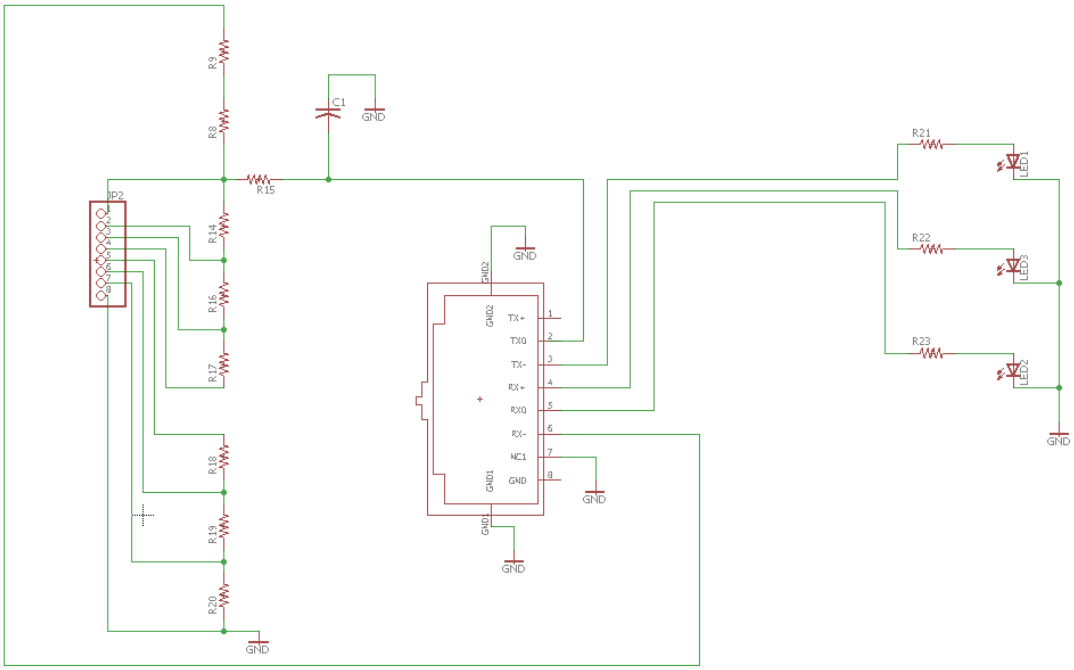


Figura H.2: Circuito Elétrico da Placa de ligação do Teclado.

O circuito da Placa de Alimentação (Figura H.1) pode ser dividido em 4 partes principais:

1. Circuito Opto-Isolador;
2. Interface de ligação à Placa de ligação do Teclado;
3. Circuito UPS (*Uninterruptible Power Supply*);
4. Conversão dos 12V de alimentação em 5V;

Circuito Opto-Isolador

O Circuito Opto-Isolador apresentado na Figura H.3 tem o objetivo de separar o trinco elétrico dos restantes componentes do sistema. A utilização deste circuito permite a proteção dos restantes componentes do sistema face a um pico de tensão ou a um possível curto-circuito.

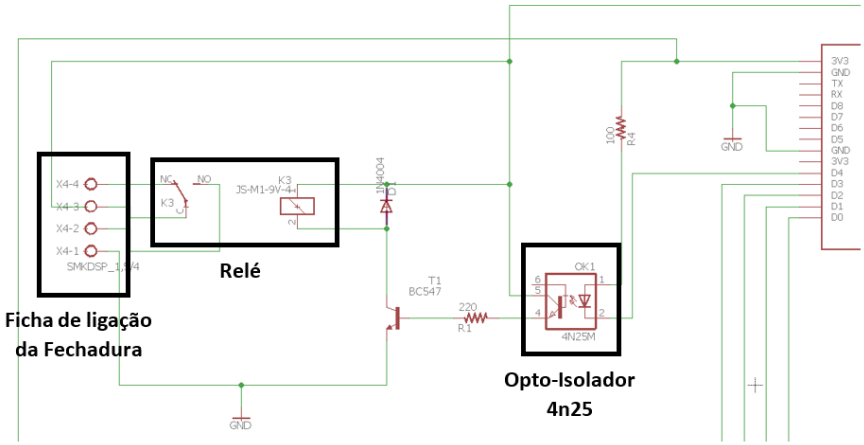


Figura H.3: Circuito Opto-Isolador.

Interface de ligação à Placa de ligação do Teclado

Com já referido no início deste apêndice, a separação dos elementos do sistema de controlo de acessos proposto tem por objetivo a prevenção de possíveis entradas indesejadas no alojamento. Dessa forma, é necessário garantir a existência de uma interface de ligação entre as duas placas.

Para o bom funcionamento da solução, é necessário garantir a passagem de 1 fio para a alimentação do teclado, 1 fio para a ligação do teclado à porta analógica, 3 fios para os LED's indicadores de "Código Certo" ou "Código Errado". Um cabo existente que contenha, pelo menos, os 5 cabos necessários para a ligação entre as duas placas é o cabo "Ethernet". Não foi considerada nenhuma informação relativa ao protocolo de comunicação "Ethernet" entre as duas placas, visto que apenas se utilizou o cabo pela quantidade de fios oferecida (Ver Figura H.4).

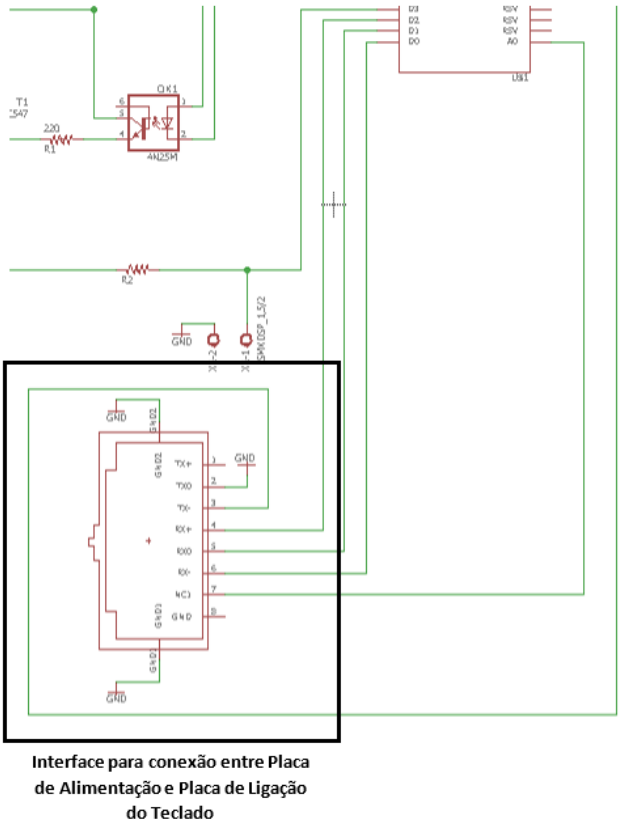


Figura H.4: Interface de ligação à Placa de ligação do Teclado.

Circuito UPS

Uma das premissas tidas em conta no desenvolvimento desta solução foi a robustez do sistema face a possíveis imprevistos no decorrer do seu funcionamento. Na eventualidade de haver uma falha de corrente na unidade hoteleira, é necessário garantir a continuidade no acesso ao alojamento. Para isso, foi prevista a instalação de uma pequena bateria de 12V que permite a alimentação do ESP e da fechadura imediatamente após o momento da falha energética. A bateria apenas é recarregada quando a energia voltar, encontrando-se sempre pronta a intervir na altura desejada (Figura H.5).

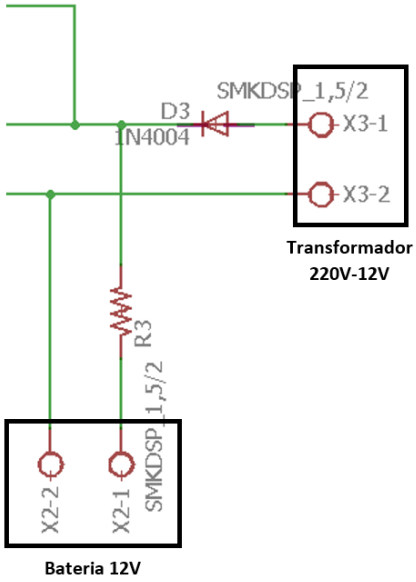


Figura H.5: Circuito UPS.

Conversão dos 12V de alimentação em 5V

Neste sistema, são necessários 2 tipos de alimentação diferentes: uma para o ESP (5V) e outra para a fechadura (12V). Para garantir apenas uma alimentação na placa desenvolvida, foi utilizado um pequeno regulador de tensão que permite a passagem dos 12V para os 5V necessários ao funcionamento do ESP. Algumas unidades hoteleiras com fechaduras elétricas já possuem cabos de 12V instalados, para a ligação direta da fechadura. Noutras instalações, a passagem dos 220V para os 12V necessários pode ser conseguida com recurso a um transformador (Figura H.6).

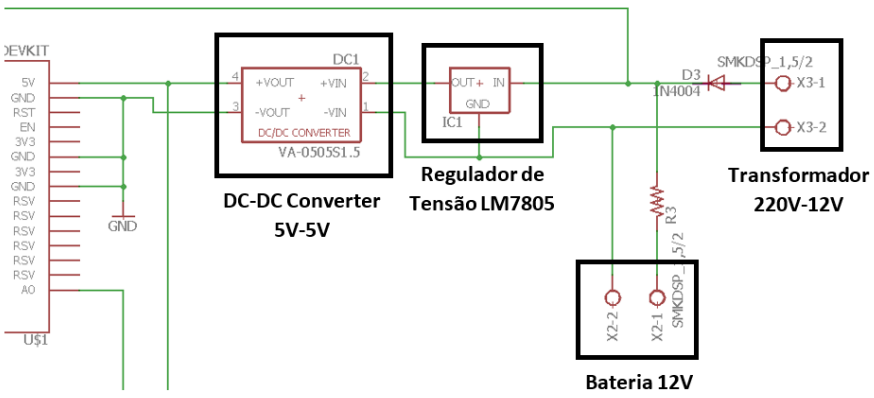


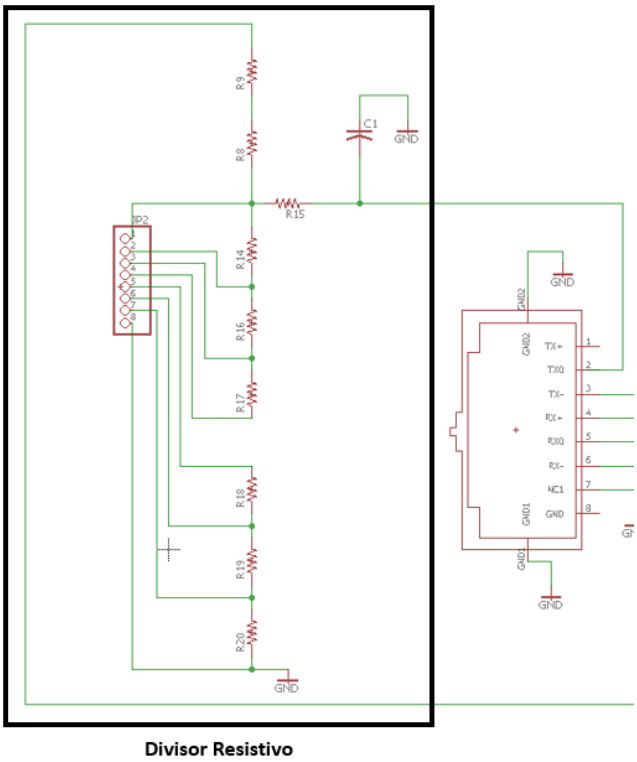
Figura H.6: Conversão dos 12V de alimentação em 5V.

A Placa de Ligação do Teclado (Figura H.2), por sua vez, encontra-se dividida em 2 partes principais:

1. Divisor Resistivo;
2. Interface de ligação à Placa de Alimentação e Comunicação (Mesmo princípio da Interface da Placa de Alimentação e Comunicação).

Divisor Resistivo

O divisor resistivo (Figura H.7), como referido no apêndice anterior, tem a funcionalidade de atribuir um valor de tensão diferente a cada tecla pressionada no Teclado. Esse valor de tensão é posteriormente lido na porta analógica e convertido em valor digital pela ADC do ESP. Para estabilizar o valor de tensão antes da entrada analógica, é utilizado um pequeno circuito RC (Filtro Passa-Baixo).



Divisor Resistivo

Figura H.7: Divisor Resistivo para leitura das Teclas.

Interface de ligação à Placa de Alimentação e Comunicação

Esta interface (Figura H.8) de ligação tem a mesma estrutura que a anterior (Figura H.4).

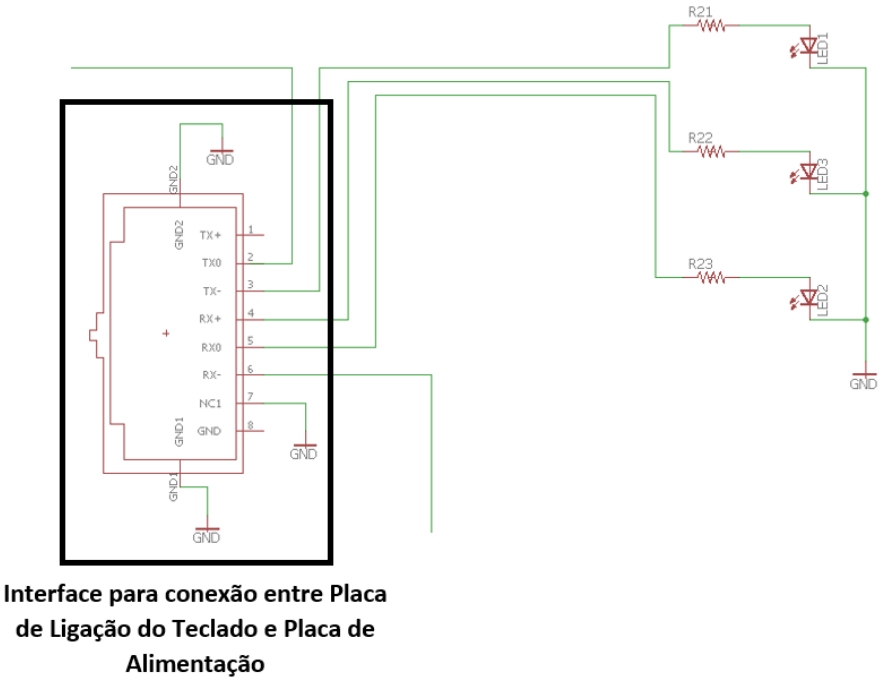


Figura H.8: Interface de ligação à Placa de Alimentação e Comunicação.